

Manual de Usuario

Modelo aplicable(s): M5F PRO

Fecha: Mayo 2025
Versión: 1.0

Gracias por elegir nuestro producto. Por favor, lea atentamente las instrucciones antes de utilizarlo. Siga estas instrucciones para asegurarse de que el p roducto funciona corre ctamente. Las imágenes mostradas en este manual son sólo para fines ilustrativos. Para más información, visite el sitio www.zkteco.com

Copyright 2020 ZKTECO CO, LTD. Todos los derechos reservados.

Sin el consentimiento previo por escrito de ZKTeco, ninguna parte de este manual puede ser copiada o reenviada de ninguna manera o forma. Todas las partes de esta manual pertenecen a ZKTeco y sus filiales (en adelante, la «Empresa» o «ZKTeco").

Marca Registrada

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

Descargo de responsabilidad

Este manual contiene información sobre el funcionamiento y el mantenimiento del equipo ZKTeco. El copyright de todos los documentos, dibujos, etc. relacionados con el equipo suministrado por ZKTeco es propiedad de ZKTeco. Su contenido no debe ser utilizado ni compartido por el receptor con terceros sin la autorización expresa y por escrito de ZKTeco.

El contenido de este manual debe ser leído en su totalidad antes de iniciar la operación y mantenimiento del equipo suministrado. Si alguno de los contenidos del manual le parece poco claro o incompleto, póngase en contacto con ZKTeco antes de iniciar el funcionamiento y mantenimiento de dicho equipo.

Un requisito previo esencial para el funcionamiento y mantenimiento satisfactorios es que el personal de funcionamiento y mantenimiento esté totalmente familiarizado con el diseño y que dicho personal haya recibido una formación completa en el funcionamiento y mantenimiento de la máquina/unidad/equipo. Además, es esencial para el funcionamiento seguro de la máquina/unidad/equipo que el personal haya leído, comprendido y seguido las instrucciones de seguridad contenidas en el manual.

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

ZKTeco no ofrece ninguna garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las modificaciones introducidas en el mismo, ZKTeco no extiende la garantía de ningún tipo, incluyendo, sin limitación, cualquier garantía de diseño, comerciabilidad o idoneidad para un propósito particular.

ZKTeco no asume responsabilidad alguna por errores u omisiones en la información o documentos a los que se hace referencia o que están vinculados a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenidos de la utilización de la información.

ZKTeco no será responsable en ningún caso ante el usuario ni ante terceros de ningún daño incidental, consecuente, indirecto, especial o ejemplar, incluyendo, sin limitación, la pérdida de negocio, la pérdida de beneficios, la interrupción de negocio, la pérdida de información comercial o cualquier pérdida pecuniaria, que surja de, en conexión con, o en relación con el uso de la información contenida en o referenciada por este manual, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños.

Este manual y la información contenida en el mismo pueden incluir imprecisiones técnicas, de otro tipo o errores tipográficos . ZKTeco modifica periódicamente la infformación aquí contenida, que se incorporará en nuevas adiciones/enmiendas al manual. ZKTeco se reserva el derecho de añadir, eliminar, enmendar o modifica r la información contenida en el manuala de vez en cuando en forma de circulares, vartas, notas, etc.

para un mejor funcionamiento y seguridad de la máquina/unidad/equipo. Dichas adiciones o modificaciones están destinadas a mejorar el funcionamiento de la máquina/unidad/equipo y dichas modificaciones no darán derecho a reclamar ninguna compensación o indemnización por daños y perjuicios en ninguna circunstancia.
ZKTeco no será responsable en ningún caso (i) en caso de mal funcionamiento de la máquina/unidad/equipo debido al incumplimiento de las instrucciones contenidas en este manual (II) en caso de funcionamiento de la máquina/unidad/equipo más allá de los límites de la tarifa (III) en caso de funcionamiento de la máquina y el equipo en condiciones diferentes a las prescritas en el manual.

El producto se actualizará de vez en cuando sin previo aviso. Los procedimientos de funcionamiento más recientes y los documentos pertinentes están disponibles en **https://www.zktecolatinoamerica.com**

Sede de ZKTeco

Dirección ZKTeco Industrial Park, No. 26, 188 Industrial Road, Tang Xia Town, Dong guan, China.

Teléfono +86 769 – 82109991

Fax +86 755 - 89602394

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

Acerca del Manual

Este manual presenta las operaciones deM5FPRO.

Todas las figuras mostradas son solo para fines ilustrativos. Las figuras de este manual pueden no corresponder exactamente a los productos reales.
Características y parámetros con ★ No están disponibles en todos los dispositivos.

Convenciones del Documento

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

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

Símbolos

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

Índice

DECLARACIÓN DE SEGURIDAD DE LOS DATOS 8

MEDIDAS DE SEGURIDAD 8

1 INSTRUCCIONES DE USO 10
- 1.1 POSICIÓN DE LOS DEDOS 10
- 1.2 POSICIÓN DE PIE, POSTURA Y EXPRESIÓN FACIAL 11
- 1.3 REGISTRO DE PLANTILLAS FACIALES 12
- 1.4 INTERFAZ DE ESPERA 14
- 1.5 TECLADO VIRTUAL 14
- 1.6 MODO DE VERIFICACIÓN 15
  - 1.6.1 VERIFICACIÓN DE HUELLAS DACTILARES 15
  - 1.6.2 VERIFICACIÓN DE TARJETAS 17
  - 1.6.3 VERIFICACIÓN FACIAL 19
  - 1.6.4 VERIFICACIÓN DE CONTRASEÑA 22
  - 1.6.5 VERIFICACIÓN COMBINADA 24

2 MENÚ PRINCIPAL 26

3 GESTIÓN DE USUARIO 28
- 3.1 REGISTRO DE USUARIO 28
  - 3.1.1 NOMBRE E ID DE USUARIO 28
  - 3.1.2 ROL DE USUARIO 29
  - 3.1.3 HUELLA 29
  - 3.1.4 PLANTILLA FACIAL 30
  - 3.1.5 TARJETA 31
  - 3.1.6 CONTRASEÑA 31
  - 3.1.7 FOTO DE PERFIL 32
  - 3.1.8 ROL DE CONTROL DE ACCESO 32
- 3.2 BUSQUEDA DE USUARIOS 33
- 3.3 EDITAR USUARIO 34
- 3.4 ELIMINAR USUARIO 35
- 3.5 ESTILO DE VISUALIZACIÓN 35

4 ROL DE USUARIO 36

5 CONFIGURACIÓN DE COMUNICACIÓN 38
- 5.1 CONFIGURACIÓN DE RED 38
- 5.2 COMUNICACIÓN SERIAL 39
- 5.3 CONEXIÓN A PC 40
- 5.4 RED INALÁMBRICA 41
- 5.5 CONFIGURACIÓN DE SERVIDOR EN LA NUBE 44
- 5.6 CONFIGURACIÓN WIEGAND 45
  - 5.6.1 ENTRADA WIEGAND 47
  - 5.6.1 SALIDA WIEGAND 47
- 5.7 DIAGNOSTICO DE RED 48

6 CONFIGURACIÓN DEL SISTEMA 49
6.1 FECHA Y HORA 50
6.2 CONFIGURACIÓN DE REGISTROS DE ASISTENCIA/ACCESO 51
6.3 PARÁMETROS DE PLANTILLA FACIAL 54
6.4 PARÁMETROS DE HUELLA DIGITAL 57
6.5 CONFIGURACIÓN DE TIPO DE DISPOSITIVO 58
6.6 CONFIGURACIÓN DE SEGURIDAD 59
6.7 ACTUALIZACIÓN POR USB 60
6.8 ACTUALIZACIÓN DE FIRMWARE EN LÍNEA 60
6.9 RESTABLECER DE FÁBRICA 61

7 CONFIGURACIÓN DE PERSONALIZACIÓN 62
7.1 CONFIGURACIÓN DE INTERFAZ DE USUARIO 62
7.2 CONFIGURACIÓN DE VOZ 63
7.3 HORARIOS DE CAMPANA 63
7.4 OPCIONES DE ESTADOS DE MARCAJE 65
7.5 MAPEOS DE TECLAS DE ACCESO RÁPIDO 66

8 GESTIÓN DE DATOS **68**
8.1 ELIMINAR DATOS 68

9 CONTROL DE ACCESO **70**
9.1 OPCIONES DE CONTROL DE ACCESO 71
9.2 HORARIO/REGLAS DE TIEMPO 74
9.3 HORARIOS 75
9.4 GRUPOS DE ACCESO 76
9.5 VERIFICACIÓN COMBINADA 77
9.6 CONFIGURACIÓN DE ANTIPASSBACK 78
9.7 OPCIONES DE COACCIÓN 79

10 GESTOR USB **81**
10.1 DESCARGA USB 81
10.2 CARGA USB 82
10.3 OPCIONES DE DESCARGA 83

11 BÚSQUEDA DE ASISTENCIA **84**

12 AUTOTEST **86**

13 INFORMACIÓN DEL SISTEMA **87**

14 CONEXIÓN AL SOFTWARE EN LA NUBE BIOTIME **88**
10.1 AGREGAR DISPOSITIVO EN EL SOFTWARE 88
10.2 AGREGAR PERSONAL EN EL SOFTWARE 89

15 CONEXIÓN AL SOFTWARE ZKBIO CVACCESS 90
15.1 CONFIGURAR DIRECCIÓN DE COMUNICACIÓN.....90
15.2 AGREGAR DISPOSITIVO EN EL SOFTWARE.....90
15.2 AGREGAR PERSONAL EN EL SOFTWARE 92

APÉNDICE 1 93
REQUISITOS PARA RECOLECCIÓN Y REGISTRO DE PLANTILLAS FACIALES DE LUZ VISIBLE.....93
REQUISITOS PARA DATOS DIGITALES DE PLANTILLAS FACIALES DE LUZ VISIBLE.....94

APÉNDICE 2 95
POLÍTICA DE PRIVACIDAD 95

FUNCIONAMIENTO ECOLÓGICO..... 97

Declaración de seguridad de datos

ZKTeco, como proveedor de productos inteligentes, también puede necesitar conocer y recopilar parte de su información personal para ayudarlo mejor a utilizar los bienes y servicios de ZKTeco, y tratará su privacidad con cuidado mediante el desarrollo de una Política de privacidad.
Lea y comprenda completamente todas las normas de política de protección de la privacidad y los puntos clave que aparecen en el dispositivo antes de utilizar los productos ZKTeco.
Como usuario del producto, debe cumplir con las leyes y regulaciones aplicables relacionadas con la protección de datos personales al recopilar, almacenar y utilizar datos personales, lo que incluye, entre otros, tomar medidas de protección para los datos personales, como realizar una gestión de derechos razonable para los dispositivos, fortalecer la seguridad física de los escenarios de aplicación del dispositivo, etc.

Medidas de seguridad

Las siguientes precauciones son para garantizar la seguridad del usuario y evitar daños. Léalas atentamente antes de la instalación.

1.Lea, siga y conserve las instrucciones-Todas las instrucciones de seguridad y funcionamiento deben leerse y seguirse correctamente antes de poner el dispositivo en servicio.
2.No ignore las advertencias- Respete todas las advertencias que aparecen en la unidad y en las instrucciones de funcionamiento.
3.Accesorios-Utilice únicamente los accesorios recomendados por el fabricante o los que vende el producto. No utilice ningún otro componente que no sean los materiales recomendados por el fabricante.
4.Precauciones para la instalaciónNo coloque este dispositivo sobre un soporte o marco inestable. Podría caerse y causar lesiones graves a personas y daños al dispositivo.
5.Servicio-No intente reparar esta unidad usted mismo. Abrir o quitar las cubiertas puede exponerlo a voltajes peligrosos u otros peligros.
6.Daños que requieren servicio-Desconecte el sistema de la fuente de alimentación principal de CA o CC y consulte al personal de servicio en las siguientes condiciones:

- Cuando el control del cable o de la conexión se ve afectado.
- Cuando se derramó líquido o cayó algún objeto en el sistema.
- Si el sistema está expuesto al agua y/o a condiciones climáticas adversas (lluvia, nieve, etc.).
- Si el sistema no funciona normalmente según las instrucciones de funcionamiento.

Simplemente cambie los controles definidos en las instrucciones de funcionamiento. El ajuste incorrecto de otros controles puede causar daños y requerir la intervención de un técnico cualificado para que el dispositivo vuelva a funcionar con normalidad.

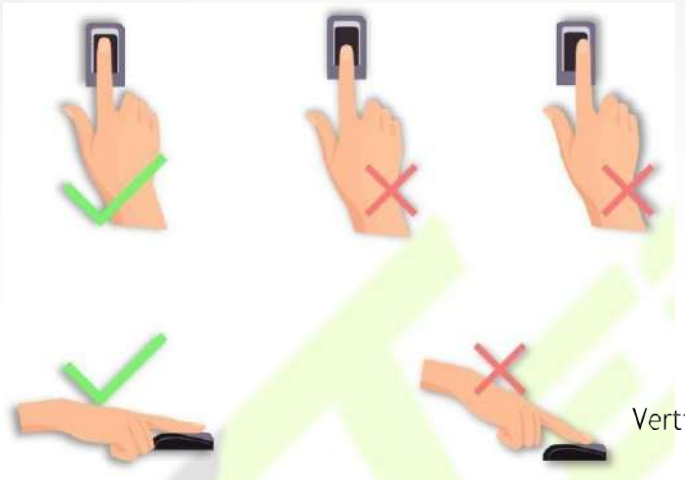
7.Piezas de repuesto-Cuando se requieran piezas de repuesto, los técnicos de servicio solo deben utilizar las proporcionadas por el proveedor. El uso de piezas de repuesto no autorizadas puede provocar quemaduras, descargas eléctricas u otros peligros.
8.Comprobación de seguridad-Al finalizar el trabajo de servicio o reparación en la unidad, solicite al técnico de servicio que realizar comprobaciones de seguridad para garantizar el correcto funcionamiento de la unidad.
9.Fuentes de energía-Utilice el sistema únicamente con la fuente de alimentación indicada en la etiqueta. Si no está claro qué tipo de fuente de alimentación debe usar, llame a su distribuidor.
10.Iluminación–Se pueden instalar pararrayos externos para protegerse contra tormentas eléctricas. Esto evita que los sobretensiones dañen el sistema.
Los dispositivos deben instalarse en áreas con acceso limitado.

1 Instrucciones de uso

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

1.1 Posición del dedo

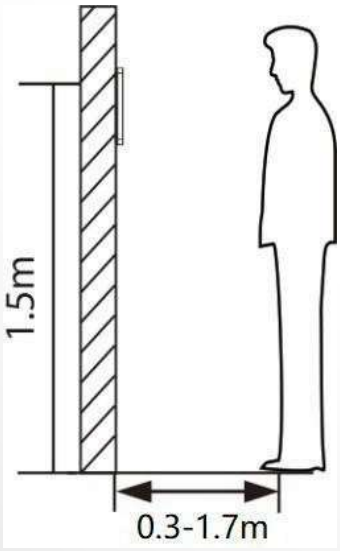
Dedos recomendados: Se recomienda utilizar el índice, el medio o el anular. Evite usar el pulgar o el meñique, yaquesondifícilesdeposicionar correctamente en el lector de huellas dactilares.



Nota: *Utilice el método correcto para presionar sus dedos sobre el lector de huellas dactilares para el registro e identificación. Nuestra empresa no se hace responsable de los problemas de reconocimiento que puedan surgir debido al uso incorrecto del producto, Nos reservamos al derecho de interpretación final y modificación respecto a este punto*

1.2 Posición de pie, postura y expresión facial

la distancia recomendada



Se recomienda que la distancia entre el dispositivo y un usuario cuya altura esté en el rango de 1,55 ma 1,85 m sea de 0,3 ma 1,7
m. Los usuarios pueden moverse ligeramente hacia adelante o hacia atrás para mejorar la calidad de las imágenes faciales capturadas.



Nota: Durante el registro y la verificación, mantenga una expresión facial y una postura de pie natural.

1.3 Registro de plantilla facial

Por favor, asegúrese de que la plantilla facial esté en el centro de la pantalla durante el registro. Mire hacia la cámara y permanezca quieto durante el registro de la plantilla facial. La pantalla debe verse como la imagen a continuación:



Método correcto de registro y autenticación de la plantilla facial

Recomendaciones para registrar una plantilla facial

- Al registrar una plantilla facial, mantenga una distancia de 40 cm a 80 cm entre el dispositivo y la plantilla facial.

- Tenga cuidado de no cambiar su expresión facial. (Plantilla facial sonriendo, plantilla facial dibujada, guiño, etc.)
- Si no sigue las instrucciones en la pantalla, el registro de la plantilla facial puede tardar más o puede fallar.
- Tengacuidadodenocubrir losojoso lascejas.
- No use sombreros, máscaras, gafas de sol o anteojos.
- Tenga cuidado de no mostrar dos plantillas faciales en la pantalla. Registre una persona a la vez.

Recomendaciones para autenticar una plantilla facial

- Asegúrese de que la plantilla facial esté dentro de la guía que aparece en la pantalla del dispositivo.
- Si se han cambiado las gafas, la autenticación puede fallar. Si se ha registrado la plantilla facial sin gafas, autentique la plantilla facial sin gafas. Si se han registrado la plantilla facial con gafas, autentique la plantilla facial con las gafas previamente usadas.
- Si una parte de la plantilla facial está cubierta por un sombrero, una mascara, un parche ocular o gafas de sol, la autenticación puede fallar, No cubra la plantilla facial, permita que el dispositivo reconozca tanto las cejas como la plantilla facial.

1.4 Interfaz de espera

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

- Haga clic en el ícono para ingresar a la plantilla de interfaz de entrada del ID de usuario.



- Cuando no haya un Super Administrador configure el dispositivo, toque el ícono para ir al menú.

- Después de configurar el Super Administrador en el dispositivo, se realizará la verificación del Super Administrador antes de ingresar a las funciones del menú

Nota: Por razones de seguridad del dispositivo, se recomienda registrar al Super Administrador la primera vez que utilice el dispositivo.

- En la plantilla de la interfaz de espera, las opciones de estado de asistencia también pueden mostrarse y usarse directamente. Haga clic en cualquier parte de la pantalla, excepto en los íconos, y aparecerán seis



- Presione la tecla correspondiente al estado de asistencia para seleccionar su estado actual, el cual se mostrará en verde.

Nota: Las opciones de estado de asistencia están desactivadas por defecto y deben cambiarse a otra opción en el "7.5 Asignación de teclas de acceso rápido"para que las opciones de estado de asistencia aparezcan en la pantalla de espera.

1.5 Teclado Virtual



Nota:
El dispositivo admite la entrada en idioma chino, idioma inglés, números y símbolos

- Haga clic en EN para cambiar al teclado en inglés
- Presione 123 para cambiar al teclado numérico y de símbolos.
- Haga clic en @#& para regresar al teclado alfabético.
- Haga clic en el cuadro de entrada para que aparezca el teclado virtual.
- Haga clic para salir del teclado virtual.

1.6 Modo de verificación

1.6.1 Verificación de Huellas dactilares

-1: Modo de verificación de huellas dactilares
El dispositivo compara la huella dactilar actual con los datos de huellas dactilares disponibles almacenados en su base de datos.
El modo de autenticación de huellas dactilares se activa cuando un usuario coloca su dedo en el escáner de huellas dactilares.
Siga la forma recomendada para colocar el dedo en el sensor. Para obtener más información, consulte sección **Posicionamiento de los dedos.**

La verificación se ha realizado correctamente:



Se ha producido un error en la verificación:



-1:1Modo de verificaciónondehuellas dactilares

El dispositivo compara la huella digital actual con las huellas dactilares vinculadas al ID de usuario ingresado a través del teclado virtual
En caso de que los usuarios no puedan obtener acceso mediante el método de autenticación 1:N, pueden intentar verificar su identidad mediante el modo de verificación 1:1.

Haga clic en el botón de la pantalla principal para ingresar al modo de verificación de huellas dactilares introduzca el ID de usuario y pulse DE ACUERDO.

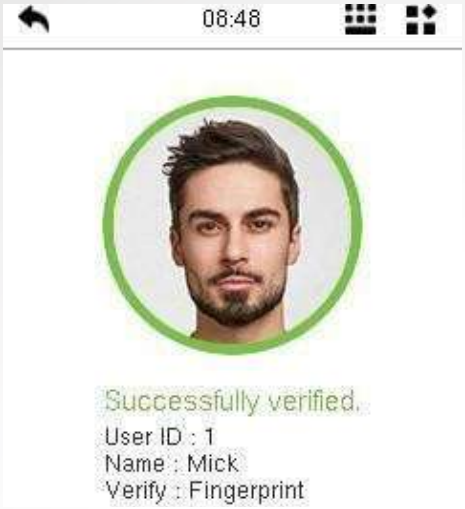


Si el usuario tiene una plantilla de rostro, una tarjeta y una contraseña registradas además de sus huellas dactilares y el método de verificación está configurado como Verificación de contraseña/ huella dactilar/tarjeta/ plantilla de rostro, aparecerá la siguiente pantalla. Seleccione el icono de huella dactilar para ingresar al modo de verificación de huellas dactilares.



Presione la huella digital para verificar.

La verificación se ha realizado correctamente:



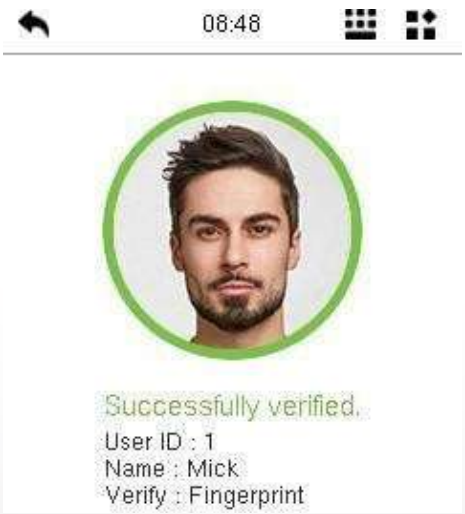
Se ha producido un error en la verificación:



1.6.2 Verificación con tarjeta

-1:N Verificación de la tarjeta

El modo de verificación de tarjeta 1:N compara el número de tarjeta en el área de inducción de la tarjeta con todos los datos del número de tarjeta registrados en el dispositivo; En la verificación de la tarjeta se muestra la siguiente pantalla:



-1:1 Verificación de la tarjeta

El modo de verificación de tarjeta 1:1 compara el número de tarjeta en el área de inducción de tarjetas con el número asociado con el ID de usuario del empleado registrado en el dispositivo.
Presione en la plantilla de la interfaz principal para abrir el modo de verificación de tarjeta 1:1. Introduce el ID de usuario y haz clic enAceptar.

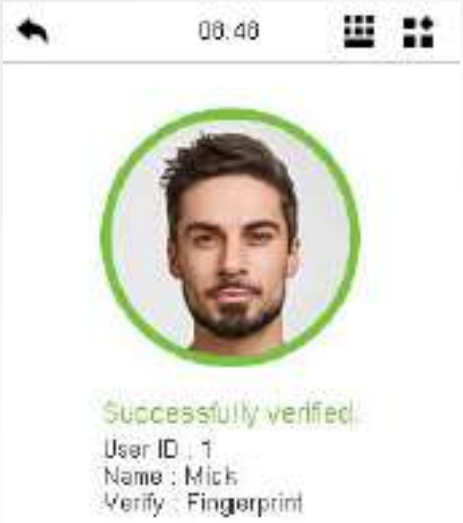


Si el usuario tiene una plantilla de rostro registrado, una tarjeta y una contraseña además de su tarjeta, y el método de verificación está configurado en Contraseña / Huella digital / Tarjeta / Verificación facial, aparecerá la siguiente pantalla. Seleccione el icono para ingresar al modo de verificación de la tarjeta.

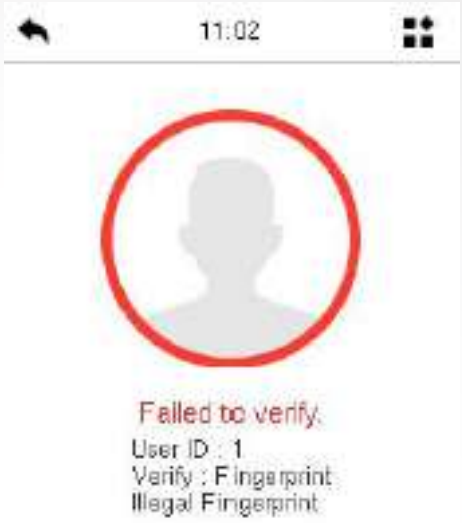


Coloque la tarjeta en el área de recolección para su verificación.

La verificación se ha realizado correctamente:



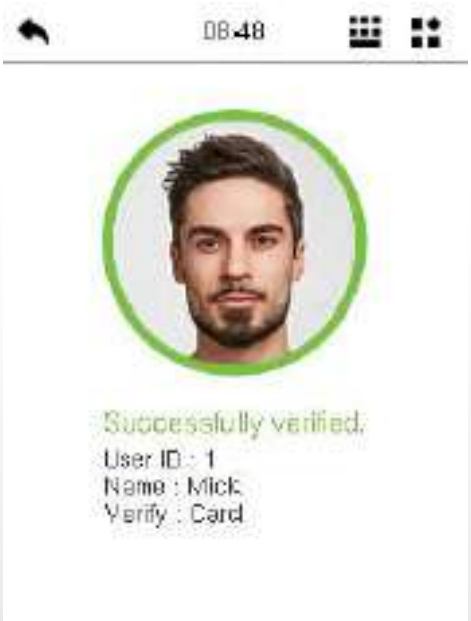
Se ha producido un error en la verificación:



1.6.3 Verificación facial

-1:N Verificación facial

El dispositivo compara las imágenes faciales adquiridas actualmente con todos los datos de plantillas faciales registradas almacenadas en su base de datos. A continuación se muestra el cuadro emergente que muestra el resultado de la comparación.



-Verificación facial 1:1

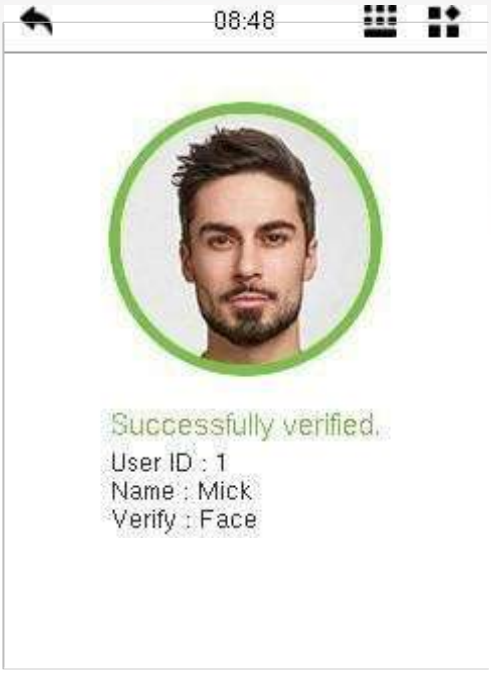
En este modo de verificación, el dispositivo compara la plantilla facial capturada por la cámara con la plantilla facial relacionada con el ID de usuario ingresado. Presione el icono en la plantilla de la interfaz principal e ingrese al modo de verificación facial 1:1 e ingrese el ID de usuario y haga clic en Aceptar.



Si el usuario ha registrado una tarjeta, huella dactilar y contraseña además de su plantilla de rostro, y el método de verificación está configurado en Verificación de contraseña/huella dactilar/tarjeta/ rostro, aparecerá la siguiente pantalla. Seleccione el icono para entrar en el modo de verificación de la plantilla facial.



Después de una verificación exitosa, el cuadro de aviso mostrará "Verificado exitosamente", como se muestra a continuación:



Si se produce un error en la verificación, se le solicita "¡Por favor, ajuste su posición!".

1.6.4 Verificación de contraseña

El dispositivocompara lacontraseña introducida con lacontraseña registradapor el IDdeusuariodado.
Haga clic en el botón de la pantalla principal para ingresar al modo de verificación de contraseña 1:1. A continuación, introduzca el ID de usuario y pulse DE ACUERDO.



Si el usuario ha registrado la plantilla de cara y la tarjeta además de contraseña, y el método de verificación se establece en Contraseña/Huella digital/Tarjeta/Verificación de cara, aparecerá la siguiente pantalla. Seleccione el icono para entrar en modo de verificación de contraseña.



Ingrese la contraseña y presione DE ACUERDO.



Las siguientes pantallas, después de ingresar una contraseña correcta y una contraseña incorrecta respectivamente.

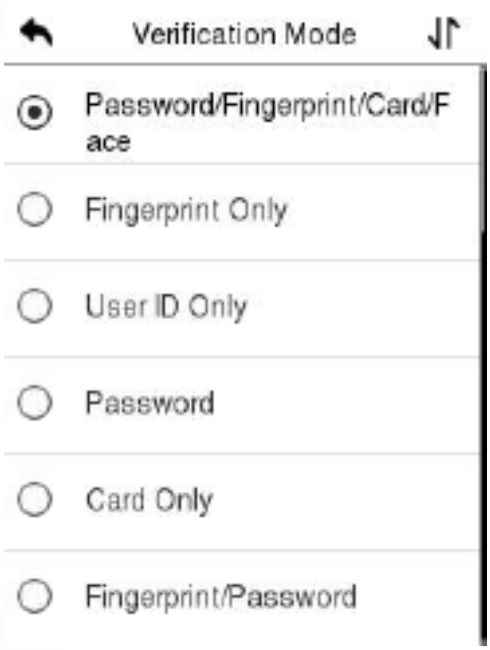




1.6.5 Verificación de verificación

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de métodos de verificación. Se pueden utilizar un total de 21 combinaciones de verificación diferentes, como se muestra a continuación:
Símbolo y definición de combinación de verificación:

Simbólo	Definición	Explicación
/	o	Este método compara la verificación ingresada de una persona con la plantilla de verificación relacionada previamente almacenada en ese ID de personal en el dispositivo.
+	y	Este método compara la verificación ingresada de una persona con toda la plantilla de verificación almacenada previamente en esa identificación personal en el dispositivo.









Procedimiento para configurar el modo de verificación combinada:

- La verificación combinada requiere que el registro personal sea todos los diferentes métodos de verificación. De lo contrario, los empleados no podrán verificar con éxito el proceso de verificación combinado.

- Por ejemplo, cuando un empleado ha registrado solo los datos, pero el modo de verificación del dispositivo está configurado como "Rostro + Contraseña", el empleado no podrá completar el proceso de verificación con éxito.

- Esto se debe a que el Dispositivo compara la plantilla de rostro escaneada de la persona con la plantilla de verificación registrada (tanto la plantilla de rostro como la contraseña) almacenada previamente con ese ID de personal en el dispositivo.

- Pero como el empleado solo ha registrado la plantilla de cara pero no la contraseña, la
- verificación no se completará y el dispositivo mostrará "Error de verificación".

2 Menú Principal

Presione ☰ en la interfaz de espera para ingresar al menú principal, se mostrará la siguiente pantalla:



Descripción de la función

Menú	Descripciones
Administración de usuarios.	Para agregar, editar, ver y eliminar información básica de un usuario.
Rol de usuario	Para establecer el alcance de permisos del rol personalizado y el registrador para los usuarios, es decir, los derechos para operar el sistema.
Comunicación	Para establecer los parámetros relevantes de red, comunicación en serie, conexión a PC, red inalámbrica, servidor en la nube, wiegand y diagnóstico de red.
Sistema	Para establecer los parámetros relacionados con el sistema, incluida la fecha y hora, la configuración de los registros de asistencia / acceso, la plantilla facial y los parámetros de huellas dactilares, la configuración del tipo de dispositivo, la configuración de seguridad, la actualización de USB, la actualización del firmware en línea y el restablecimiento de fábrica.
Personalizar	Esto incluye la interfaz de usuario, la voz, los horarios de campanas, las opciones de estado de perforación y la configuración de asignaciones de teclas de acceso directo.
Administración de datos	Para eliminar todos los datos relevantes del dispositivo.
Intercomunicado	Para establecer los parámetros relacionados con SIP y NVR.
Control de acceso	Para establecer los parámetros de la cerradura y el dispositivo de control de acceso correspondiente, se incluyen opciones como la configuración de la regla de tiempo/ programación de tiempo, la configuración de vacaciones, los grupos de acceso, la verificación de combinación, la configuración anti-passback y la configuración de opciones decoacción.

Administrador USB	Para cargar o descargar los datos específicos mediante una unidad USB.
Búsqueda de asistencia	Para consultar los registros de eventos especificados, consulte las fotos de asistencia y las fotos de asistencia de la lista de bloqueo.
Prueba	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, el audio, el micrófono, la cámara, el sensor de huellas dactilares y el reloj en tiempo real.
Información del sistema	Para ver la capacidad de datos, la información del dispositivo y el firmware y la política de privacidad del dispositivo.

Nota: Cuando los usuarios utilizan el producto por primera vez, deben operarlo después de establecer privilegios de administrador. Toque Usuario Mgt. para agregar un administrador o editar permisos de usuario como superadministrador. Si el producto no tiene una configuración de administrador, el sistema mostrará un símbolo del sistema de configuración de administrador cada vez que ingrese al menú del dispositivo.



3 Gestión de usuarios

3.1 Registro de usuarios

Haga clicAdministrador de usuarios.En el menú principal.



3.1.1 ID de Usuario y nombre

Pulsa Nuevo usuario. Introduzca el ID del Usuario



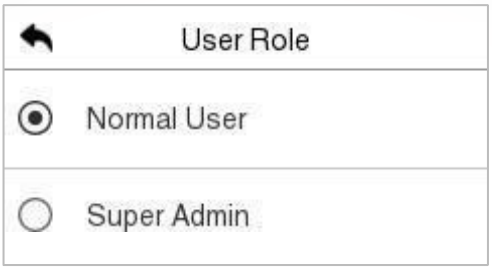
Notas:

- Un nombre de usuario puede contener un máximo de 34 caracteres.
- El ID de usuario puede contener de 1 a 14 dígitos de forma predeterminada.
- Durante el registro inicial, puede modificar su ID, que no se puede modificar después del registro.
- Si aparece el mensaje "¡¡Duplicado!", debe elegir otro ID ya que el ID de usuario ingresado ya existe.

3.1.2 Rol de usuario

En la nueva interfaz de usuario, toque Rolde usuariopara establecer el rol del usuario comoUsuario normal o Superadministrador.

- Superadministrador:El superadministrador posee todos los privilegios de gestión del dispositivo.
- UsuarioNormal:Si el Superadministrador ya está registrado en el Dispositivo, entonces los Usuarios Normales no tendrán los privilegios para administrar el sistema y solo podrán acceder a las verificaciones de autenticación.
- Roles definidos por el usuario:Elusuarionormal tambiénsepuedeconfigurarconel roldefinidoporelusuario,-quesonlosrolespersonalizadosquesepuedenestablecerparaelusuarionormal.



Nota:Si el rol de usuario seleccionado es el Super Admin, el usuario debe pasar la autenticación de identidad para acceder al menú principal. La autenticación se basa en los métodos de autenticación que el superadministrador ha registrado. Consultar1.6 Modo de verificación.

3.1.3 Huellas

Haga clic enHuella digitalpara ingresar a la página de registro de huellas dactilares. Seleccione el dedo que se va a inscribir.



Presione el mismo dedo en el lector de huellas dactilares tres veces. El verde indica que la huella digital se registró correctamente.



3.1.4 Plantilla de rostro

Toque Face en la interfaz de usuario nueva para entrar en la página de registro de plantillas de cara.

- Por favor, mire hacia la cámara y coloque su plantilla de cara dentro de la caja blanca de guía y permanezca inmóvil durante el registro de la plantilla de cara.
- Una barra de progreso aparece al registrar la plantilla de cara y un "Enrolled Successfully" se muestra a medida que la barra de progreso completa.
- Si la plantilla de cara ya está registrada entonces, aparece el mensaje "Face Duplicate". La interfaz de registro es la siguiente:



3.1.5 Tarjeta

Toque Tarjeta en la nueva interfaz deusuariopara ingresar a la página de registro de la tarjeta.

- En la interfaz de la tarjeta, deslice la tarjeta por debajo del área de lectura de la tarjeta. El registro de la tarjeta se realizará correctamente.
- Si la tarjeta ya está registrada, aparece el mensaje "Tarjeta duplicada". La interfaz de registro es la siguiente:



3.1.6 Contraseña

Toque Contraseña en la interfaz de Nuevo Usuario para ingresar a la página de registro de contraseña.

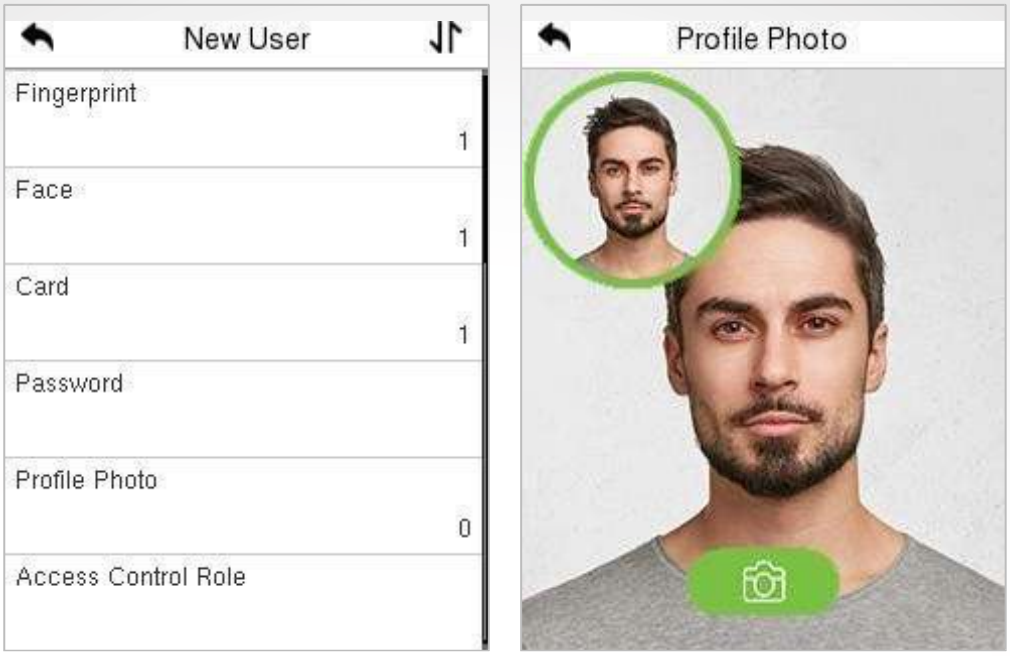
- En la interfaz de Contraseña, ingrese la contraseña requerida y vuelva a ingresarla para confirmarla, luego toque DE ACUERDO.
- Si la contraseña ingresada nuevamente es diferente de la contraseña ingresada inicialmente, el dispositivo mostrará el mensaje "¡Contraseña no coincide!", donde el usuario debe confirmar la contraseña nuevamente.



Nota: La contraseña puede contener de 6 a 8 dígitos por defecto

3.1.7 Foto de Perfil

Toca la Foto de Perfil en la interfaz de Nuevo Usuario para ir a la página de registro de Foto de Perfil



- Cuando un usuario registrado con una foto pasa la autenticación, se mostrará la foto registrada.
- Toca la Foto de Perfil, se abre la cámara del dispositivo, luego toca el ícono de la cámara para tomar una foto. La foto capturada se mostrará en la esquina superior izquierda de la pantalla y la cámara se abrirá nuevamente para tomar una nueva foto, después de
- tomar la foto inicial.

Nota:Al registrar una plantilla facial, el sistema captura automáticamente una foto como la foto de perfil del usuario. Si no registra una foto de perfil, el sistema establece automáticamente la foto capturada durante el registro como la foto predeterminada.

3.1.8 Rol de control de acceso

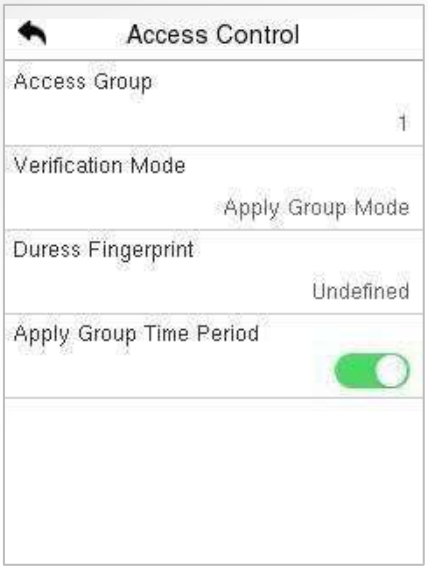
El Rol de Control de Acceso establece el privilegio de acceso a la puerta para cada usuario. Esto incluye el grupo de acceso, la huella dactilar en caso de coacción y facilitar la
configuración del período de acceso del grupo.

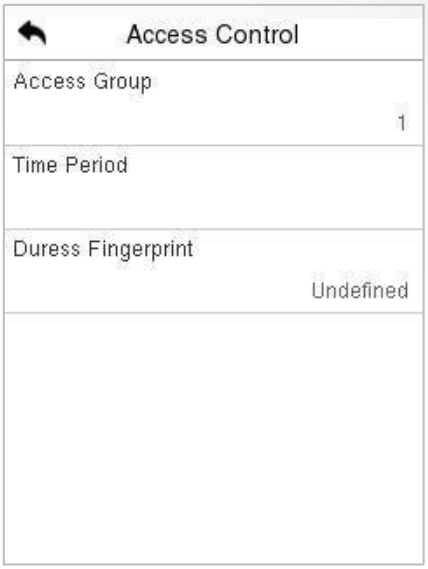
- Toca Rol de Control de Acceso > Grupo de Acceso, para asignar a los usuarios registrados a diferentes grupos y así facilitar una mejor gestión. Los nuevos usuarios pertenecen por defecto al Grupo 1 y pueden ser reasignados a otros grupos. El dispositivo admite hasta 99 grupos de Control de Acceso.
- Toca Período de Tiempo para seleccionar el período que se va a utilizar.
- Para seleccionar el modo de verificación del usuario, toque Rol de Control de Acceso > Modo de Verificación.
- El usuario puede especificar una o más huellas digitales registradas como huellas de coacción. Al presionar el dedo correspondiente a una huella de coacción sobre el sensor y pasar la verificación, el sistema generará inmediatamente una alarma de coacción. Selecciona si deseas
- Aplicar el período de tiempo del grupo para este usuario. Esta opción está habilitada por defecto.

Si no se aplica el período de tiempo del grupo, será necesario

Configurar el horario de desbloqueo para este usuario. El periodo de tiempo de este usuario no afecta el período de tiempo de ningún otro miembro del grupo. Para configurar el horario de desbloqueo de este usuario, toca Aplicar Período de Tiempo del Grupo > Período de Tiempo

1. Ingresa el número del período de tiempo y toca Aceptar. Se pueden configurar hasta 50 períodos de tiempo en el dispositivo y se pueden asignar hasta tres períodos de tiempo por usuario. Para más detalles, consulta la sección Configuración del Horario.

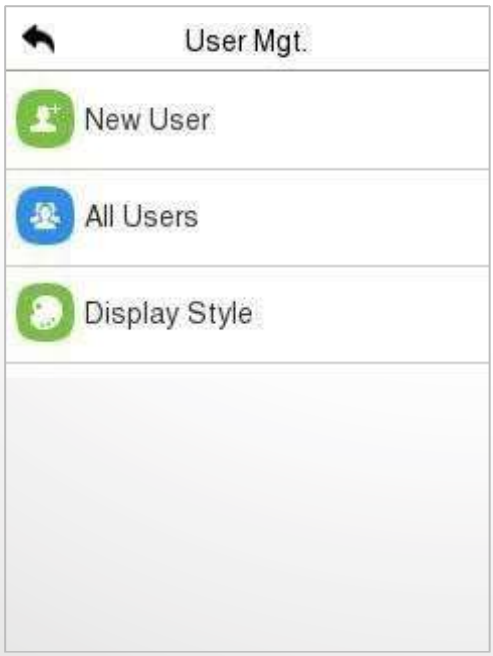




3.2 Buscar usuarios

En el Menú Principal, toque Gestión de Usuarios (User Mgt.), y luego toque Todos los Usuarios (Todos los usuarios) para buscar un usuario.

- En la interfaz de Todos los Usuarios, toque la barra de búsqueda en la lista de usuarios para ingresar la palabra clave necesaria de usuario (la cual puede ser el ID del usuario, su apellido o su nombre completo), y el sistema buscará la información del usuario relacionada.





3.3 Editar usuario

En la interfaz de Todos los Usuarios, toque el usuario deseado de la lista y luego toque Editar para modificar la información del usuario.



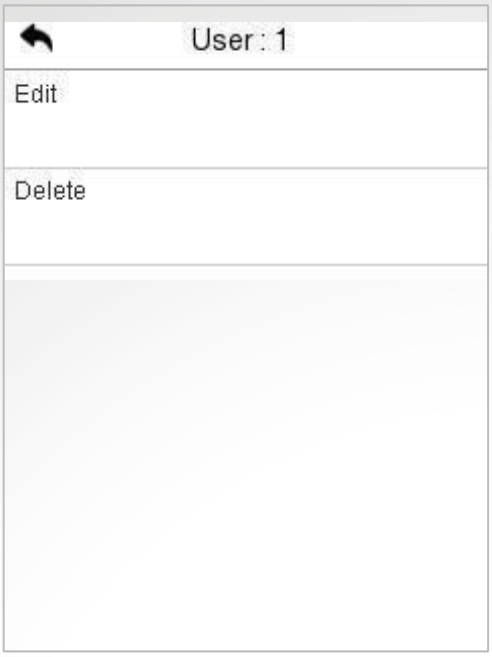
Nota:El proceso de editar un usuario es el mismo que el de agregar un usuario, con la excepción de que el ID del usuario no puede ser modificado al editar sus detalles. Para ver el proceso en detalle, consulta la sección Agregar Usuario"3. Gestión de Usuario".

3.4 Eliminar usuario

En la interfaz de Todos los Usuarios, toque el usuario deseado de la lista y luego toque Eliminar para borrar el usuario o la información específica del usuario del dispositivo. En la interfaz de Eliminar, seleccione la operación requerida y luego toque Aceptar para confirmar la eliminación.

-Operaciones de eliminación:

Eliminar usuarios: Se eliminará toda la información del usuario (elimina al usuario seleccionado por completo) del dispositivo.
Eliminar Solo Huella Digital: Eliminar la información de huella digital del usuario Seleccionado.
Eliminar Solo Rostro: Elimina la plantilla facial del usuario seleccionado.
Eliminar Solo Contraseña: Elimina la información de la contraseña del usuario seleccionado.
Eliminar Solo Número de Tarjeta: Elimina la información de la tarjeta del usuario. Seleccionado.
Eliminar solo foto de perfil: Elimina la foto de perfil del usuario seleccionado.





3.5 Estilo de visualización

Toca Gestión de Usuarios(Gestión de Usuarios)>Estilo de visualización(Estilo de Pantalla)para elegir el estilo de la lista en la interfaz de Todos los Usuarios.



Los diferentes estilos de visualización se muestran a continuación:

Múltiples:



Líneas mixtas:



4.Rol de usuario

El rol del usuariofacilitar la asignación de permisos específicos a usuarios específicos, según los requisitos

- En el Menú principal, toca Rol de usuarioy luego toca Rol definido por el usuario para configurar los permisos definidos por el usuario.
- El alcance de los permisos del rol personalizado se puede configurar hasta con 3 roles, es decir, el alcance de operación personalizado de las funciones del menú del usuario.





En la interfaz de Rol definido por el usuario, activa o desactiva Habilitar Rol Definido para habilitar o deshabilitar el rol definido por el usuario.
Toca Nombre e ingresa el nombre personalizado del rol





- Luego toca Rol Definido por el Usuarioy selecciona los privilegios que deseas asignar al nuevo rol, y después toca el botón de Regresar.
- Durante la asignación de privilegios, los nombres de las funciones del menú principal se mostrarán a la izquierda y sus submenús se listarán a la derecha.
- Primero, toque el nombre de la función del Menú principal deseado y luego selecciona los submenús correspondientes de la lista.



Nota: Si la función de Rol de Usuario está habilitada en el dispositivo, toque Gestión de Usuarios (Gestión de Usuarios) > Nuevo Usuario (Nuevo Usuario) > Rol de Usuario (Rol de Usuario) para asignar los roles creados a los usuarios requeridos.

Sin embargo, si no hay un superadministrador registrado en el dispositivo, al intentar habilitar la función de Rol de Usuario, el sistema mostrará el mensaje:
"¡Por favor registre primero un superadministrador!"

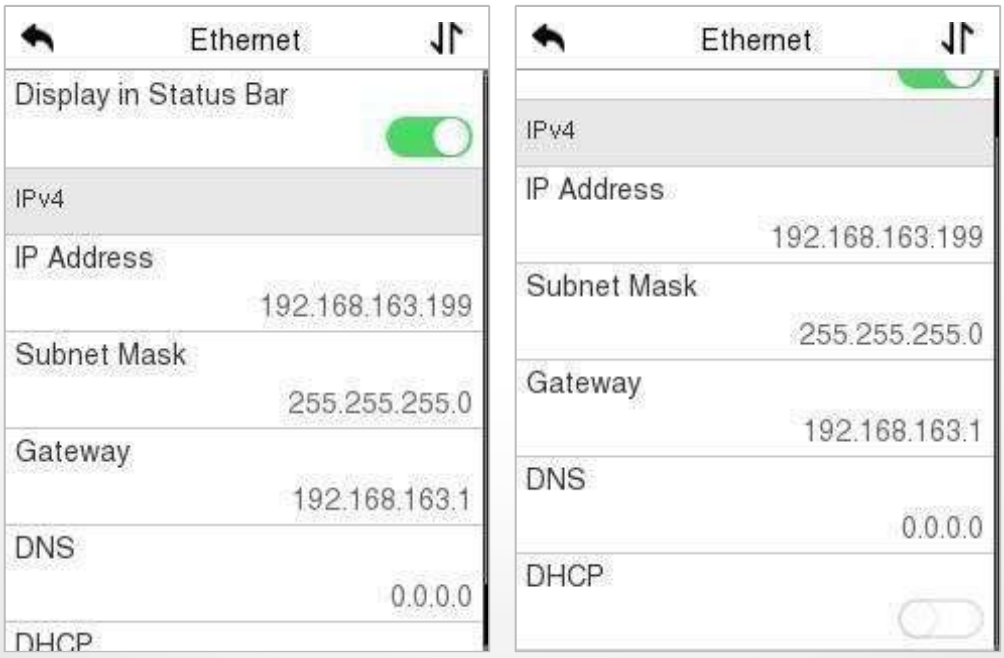
5.Configuración de comunicación

Toque COMUNIC. en el Menú Principal para configurar los parámetros correspondientes de Red, Comunicación Serial, Conexión PC, Red Inalámbrica, Servidor en la Nube, Wiegand y
Diagnóstico de Red.



5.1 Configuración de red

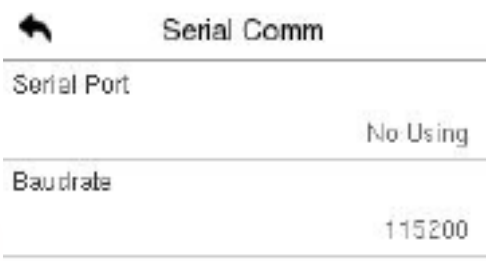
Cuando el dispositivo necesita comunicarse con una PC a través de Ethernet, es necesario configurar los ajustes de red y asegurarse de que el dispositivo y la PC estén conectados al mismo segmento de red.
Toque Ethernet en la interfaz de Configuración de Comunicación para configurar los ajustes.

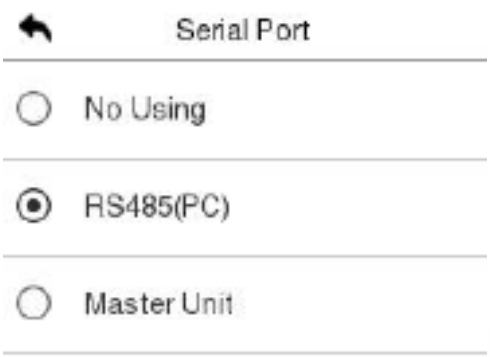


Nombre de las funciones	Descripción
Mostrar barra de estado	Seleccione si desea mostrar el icono de rojo en la barra de estado.
Dirección IP	La dirección IP por defecto es 192.168.1.201. Puede modificarse en función de la disponibilidad de la red.
Máscara de subred	La máscara de subred por defecto es 255.255.255.0. Puede modificarse en función de la disponibilidad de la red.
Puerta de enlace	La dirección de puerta de enlace por defecto es 0.0.0.0. Puede modificarse en función de la disponibilidad de la red.
DNS	La dirección DNS por defecto es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
DHCP	El protocolo de configuración dinámica de host permite asignar dinámicamente direcciones IP a los clientes a través del servidor.

5.2 Comunicación Serial

La función de comunicación serial facilita el establecimiento de comunicación con el dispositivo a través de un puerto serie (RS485/ Dispositivo maestro).
Pulse comunicación serie en la interfaz de configuración de comunicaciones





Nombre de las funciones	Descripción
Puerto Serial	No utilizar: No comunicar con el dispositivo a través del puerto serie. RS485(PC): Se comunica con el dispositivo a través del puerto serie RS485. Unidad maestra: Cuando se utiliza RS485 como la función de «Unidad maestra», el dispositivo actuará como una unidad maestra, y se puede conectar un lector de tarjetas RS485.

Velocidad en baudios	La velocidad a la que se comunican los datos con el PC, hay 4 opciones de velocidad en baudios: 115200 (por defecto), 57600, 38400 y 19200. Cuanto mayor sea la velocidad en baudios, más rápida será la velocidad de comunicación, pero también menos fiable. Por lo tanto, se puede utilizar una velocidad en baudios más alta cuando la distancia de comunicación es corta; Cuando la distancia de comunicación es larga, elegir una velocidad en baudios más baja sería más confiable.

5.3 Conexión a PC

Para mejorar la seguridad de los datos, configure una tecla de comunicación para la comunicación entre el dispositivo y el ORDENADOR PERSONAL. Es necesario introducir la contraseña de conexión antes de poder conectar el dispositivo al software de PC si se configura una clave de comunicación.

Toque Conexión a PC en la interfaz de configuración de comunicaciones para configurar los ajustes de comunicación.



Nombre de la función	Descripción
Tecla de comunicación	La contraseña predeterminada es 0 y se puede cambiar. La clave de comunicación debe tener 6 dígitos.
Identificación del dispositivo	Número de identidad del dispositivo, que oscila entre 1 y 254. Si el método de comunicación es RS232/ RS485, deberá ingresar este ID de dispositivo en la interfaz de comunicación del software.
Puerto TCP/IP	El valor predeterminado del puerto TCPCOMM es 4370. Se puede modificar según la disponibilidad de la red.
HTTPS	Para aumentar la seguridad del acceso al software, los usuarios pueden habilitar el protocolo HTTPS para crear una transmisión de red segura y cifrada, y garantizar la seguridad de los datos enviados mediante la autenticación de identidad y la comunicación cifrada. Esta función está habilitada de forma predeterminada. Esta función se puede habilitar o deshabilitar a través de la interfaz del menú, y al cambiar el estado de HTTPS, el dispositivo mostrará un mensaje de seguridad y se reiniciará después de la confirmación.

5.4 Red inalámbrica ★

El dispositivo proporciona un módulo Wi-Fi, que puede estar integrado en el molde del dispositivo o conectarse externamente.
El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (WirelessFidelity) y establece un entorno de red inalámbrica. El Wi-Fi está habilitado de forma predeterminada en el dispositivo. Si no necesita usar la red Wi-Fi, puede activar o desactivar el Wi-Fi con el botón.
Pulse Red inalámbrica en la interfaz de Ajustes dec omunicación para configurarlos ajustesde Wi-Fi.



Buscar en la red Wi-Fi

- WIFI está habilitado en el dispositivo de forma predeterminada. Botón de activación
- para activar o desactivar WIFI

Una vez activado el Wi-Fi, el dispositivo buscará el Wi-Fi disponible dentro del alcance de la red.
Elija el nombre de Wi-Fi apropiado de la listadisponible, ingrese la contraseña correcta en la interfazdecontraseña y luego toqueConectarse a Wi-Fi (Aceptar).



Wi-Fi habilitado: Toque la red requerida de la lista de redes buscadas.



Toca el campo de contraseña para introducirla y luego toca Conectar a Wi-Fi (Aceptar).

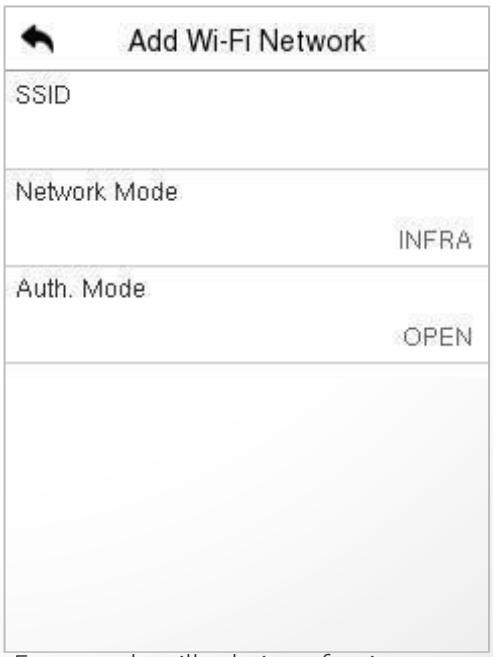
- Cuando el wifi se conecte correctamente, la interfaz inicial mostrará el Wi-Fi logo.

- Añadir Wi-Fi manualmente.

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



TapónAgregar red Wi-FiAgregar el Wi-Fi manualmente.



En esta plantilla de interfaz, ingrese los parámetros de la red Wi-Fi. (El agregado (La red debe existir).

Nota: Después de agregar correctamente la red WIFI manualmente, siga el mismo proceso para buscar el nombre de la red WIFI agregada. Haga clic aquí para ver el proceso de búsqueda de la red WIFI

- Configuración avanzada

En la interfaz de red inalámbrica, toque Avanzado para configurar los parámetros relevantes según sea necesario.





Nombre de la función	Descripción
DHCP	El protocolo de configuración dinámica de host (DHCP) asignado dinámi-camente direcciones IP a los clientes de la red. Si el DHCP está habilitado, la IP no se puede configurarla manualmente.
Dirección IP	Dirección IP para la redWi-Fi, el valor predeterminado es 0.0.0.0. Se puede modificar según la disponibilidad de la red
Máscara de subred	La máscara de subred predeterminada de la red Wi-Fi es 255.255.255.0. Se puede modificar según la disponibilidad de la red.
Puerta de enlace	La dirección de puerta de enlace predeterminada es 0.0.0.0. Se puede modificar según la disponibilidad de la red.
DNS	La dirección DNS predeterminada es 0.0.0.0. Se puede modificar según ladisponibilidad de la red.

5.5 Configuracion del servidor en la nube

Configuración del servidor en la nube en el Com. Interfaz de configuración para conectarse con el servidor ADMS.

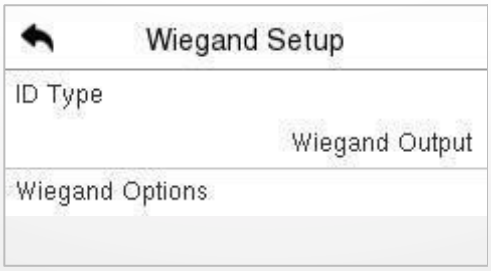


Nombre de la función	Nombre de la función	Descripción
Permitir Nombre de dominio	Dirección del servidor	Una vez habilitada esta función, se utilizará el modo de nombre de dominio "http://...", como http://www.XYZ.com, mientras que "XYZ" denota el nombre de dominio (cuando este modo está activado).
Desactivar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

5.6 Configuración de Wiegand

Para establecer los parámetros de entrada o salida Wiegand.

Configuración de Wiegand en el Com. Interfaz de configuración para configurar los parámetros de entrada o salida Wiegand.



Nota:La interfaz Wiegand es compartida y el usuario puede elegir utilizar la función de entrada Wiegand o la función de salida Wiegand para interactuar con diferentes dispositivos Wiegand.

5.6.1 Entrada Wiegand

Tipo de identificaciónen el Configuración de Wiegand, seleccionar Entrada Wiegand, y luego toque Opciones de Wieganden el Configuración de Wiegand.





Nombre de la función	Descripción
Formato Wiegand	Los valores varían entre 26 bits, 32 bits, 34 bits, 36 bits, 37 bits, 50 bits y 64 bits.
Bits Wiegand	Número de bits de datos Wiegand.
Ancho de pulso (us)	El valor del ancho de pulso enviado por Wiegand es de 100 microsegundos por defecto, el cual se puede ajustar dentro del rango de 20 a 400 microsegundos.
Intervalo de pulso (us)	El valor predeterminado es 1000 microsegundos, que se puede ajustar dentro del rango de 200 a 20000 microsegundos.
Tipo de identificación	Seleccione entre ID de usuario y número de tarjeta.

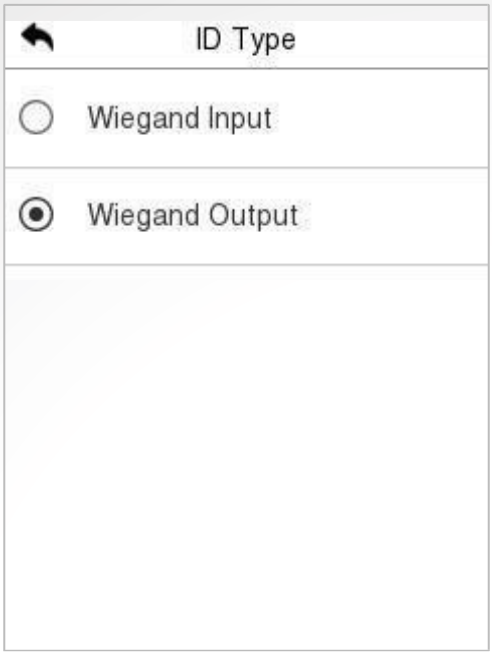
Descripción del formato Varius Common Wiegand

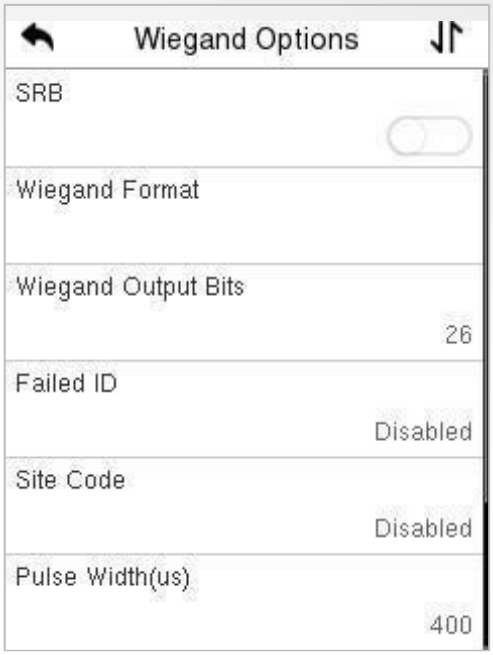
Nombre de la función	Descripción
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 13º, mientras que el 26º bit es el bit de paridad impar de los bits 14º a 25º. Los bits 2º a 25º son los números de tarjeta.

Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCO Consta de 26 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 13º, mientras que el 26º bit es el bit de paridad impar de los bits 14º a 25º. Los bits 2º a 9º son los códigos de sitio, mientras que los bits 10º a 25º son los números de tarjeta.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 17º, mientras que el 34º bit es el bit de paridad impar de los bits 18º a 33º. Los bits 2º a 25º son los números de las tarjetas.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCO Consta de 34 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 17º, mientras que el 34º bit es el bit de paridad impar de los bits 18º a 33º. Los bits 2º a 9º son los códigos de sitio, mientras que los bits 10º a 25º son los números de tarjeta.
Wiegand36	OFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El 1er bit es el bit de paridad impar de los bits 2º a 18º, mientras que el 36º bit es el bit de paridad par de los bits 19º a 35º. Los bits 2º a 17º son los códigos de dispositivo. Los bits 18º a 33º son los números de tarjeta, y los bits 34º a 35º son los códigos de fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El 1º bit es el bit de paridad par de los bits 2º a 18º, mientras que el 36º bit es el bit de paridad impar de los bits 19º a 35º. Los bits 2º a 19º son los códigos de dispositivo, y los bits 20º a 35º son los números de tarjeta.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El 1º bit es el bit de paridad impar de los bits 2º a 18º, mientras que el 37º bit es el bit de paridad par de los bits 19º a 36º. Los bits 2º a 4º son los códigos del fabricante. Los bits 5º a 16º son los códigos de sitio, y los bits 21º a 36º son los números de tarjeta.
Wiegand37a	EMMMFFFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El 1º bit es el bit de paridad par de los bits 2º a 18º, mientras que el 37º bit es el bit de paridad impar de los bits 19º a 36º. Los bits 2º a 4º son los códigos del fabricante. Los bits 5º a 14º son los códigos de dispositivo, los bits 15º a 20º son los códigos de sitio y los bits 21º a 36º son los números de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El 1er bit es el bit de paridad par de los bits 2º a 25º, mientras que el 50º bit es el bit de paridad impar de los bits 26º a 49º. Los bits 2º a 17º son los códigos de sitio, y los bits 18º a 49º son los números de tarjeta.
"C" denota el número de tarjeta; "E" denota el bit de paridad par; "O" denota el bit de paridad impar; F" denota el código de la instalación; "M" denota el código del fabricante; "P" denota el bit de paridad; y "S" denota el código del sitio.	

5.6.2 Salida Wiegand

Tipo de identificación en el Configuración de Wiegand, seleccionar Salida Wiegand, y luego toque Opciones de Wieganden el Configuración de Wiegand.





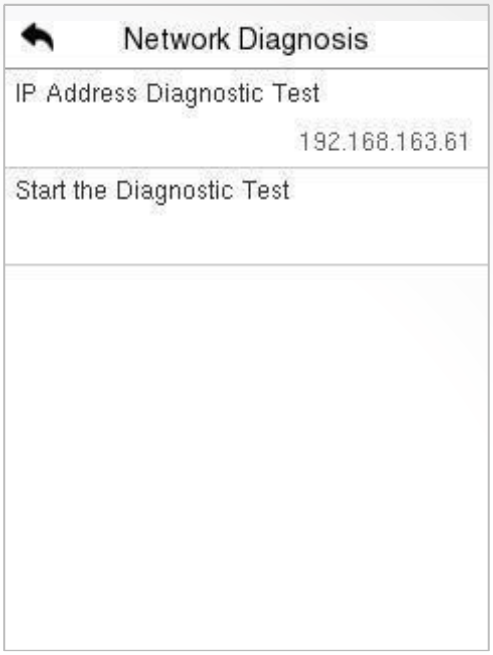
Nombre de la función	Descripción
SRB★	Cuando SRB está habilitado, el bloqueo es controlado por el SRB para evitar que se abra debido a la extracción del dispositivo.
Formato Wiegand	Los valores varían entre 26 bits, 32 bits, 34 bits, 36 bits, 37 bits y 50 bits.
Salida Wiegand Bits	Después de seleccionar el formato Wiegand requerido, seleccione los dígitos de bits de salida correspondientes del formato Wiegand.
Identificación fallida	Si la verificación falla, el sistema enviará el ID fallido al dispositivo y reemplazará el número de tarjeta o ID de personal por el nuevo.
Código del sitio	Es similar al ID del dispositivo. La diferencia radica en que el código de sitio se puede configurar manualmente y se puede repetir en un dispositivo diferente. El valor válido predeterminado es de 0 a 256.
Ancho de pulso (us)	El ancho de tiempo representa los cambios de la cantidad de carga eléctrica con capacitancia regular de alta frecuencia dentro de un tiempo específico.
Intervalo de pulso (us)	El intervalo de tiempo entre pulsos.
Tipo de identificación	Seleccione los tipos de identificación como ID de usuario o número de tarjeta.

5.7 Diagnóstico de red

Para configurar los parámetros de diagnóstico de red.

Diagnóstico de red en el Com. Interfaz de configuración para establecer el diagnóstico de la dirección IP e iniciar los parámetros de diagnóstico.





6 Configuración del Sistema

Establecer parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.

Sistema en el Menú principal Interfaz para configurar los parámetros del sistema relacionados para optimizar el rendimiento del dispositivo.
Terminal de control de asistencia:



Terminal de control de acceso:



6.1 Fecha y hora

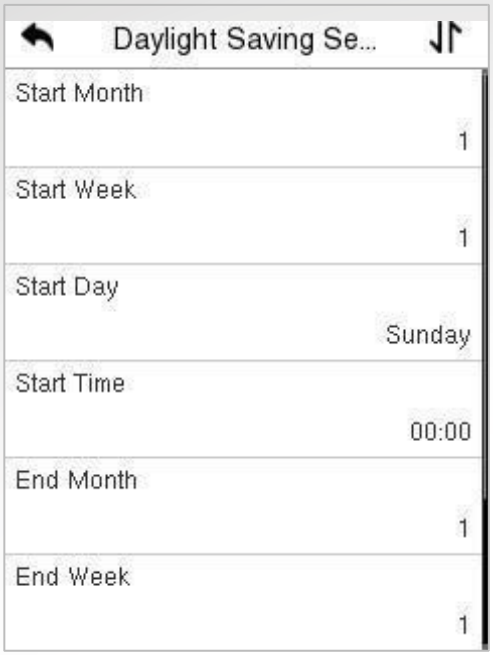
Fecha y hora en el Sistema Interfaz para configurar la fecha y la hora.



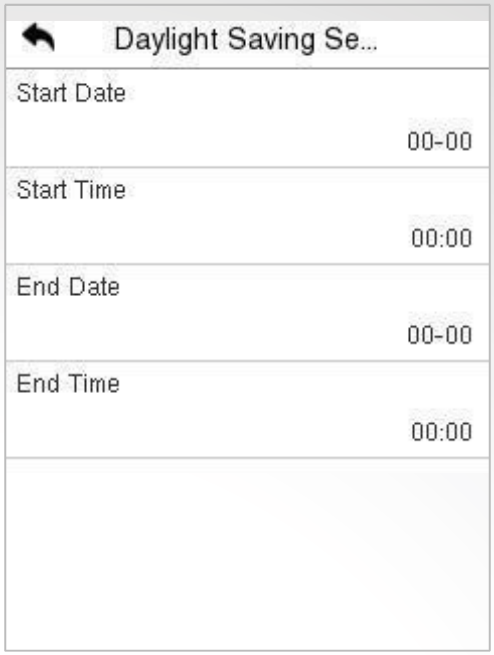
- El producto admite el sistema de sincronización horaria NTP de forma predeterminada. Esta función se activa después de...Servidor NTP está habilitado y se establece el enlace de dirección del servidor NTP correspondiente.
- Si los usuarios necesitan configurar la fecha y la hora manualmente, deshabilíteloServidor NTP primero y luego toque Manual de datos y tiempo Para establecer fecha y hora y pulsar Confirmar para salvar.



- 24 horas Para habilitar o deshabilitar este formato. Si está habilitado, seleccione Formato de fecha para establecer el formato de fecha.
- Horario de verano Para habilitar o deshabilitar la función. Si está habilitada, toque Modo de ahorro de luz diurna para seleccionar un modo de horario de verano y luego toque Configuración del horario de verano para configurar el interruptor



Modo semana



Modo de fecha

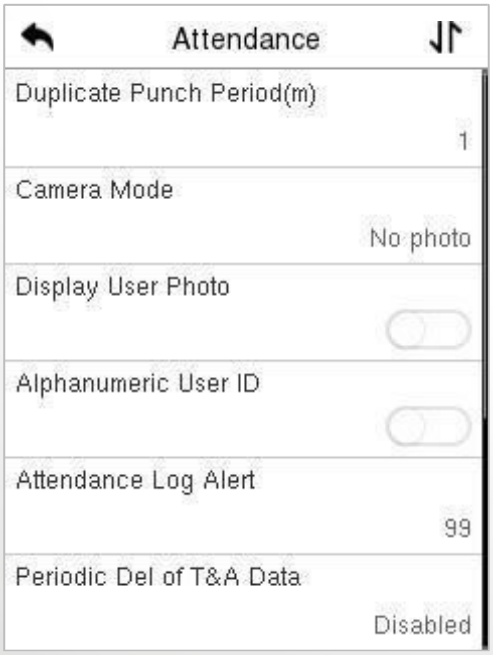
- Al restaurar la configuración de fábrica, se puede restaurar el formato de hora (24 horas) y fecha (AAAA-MM-DD), pero no se puede restaurar la fecha y la hora del dispositivo.

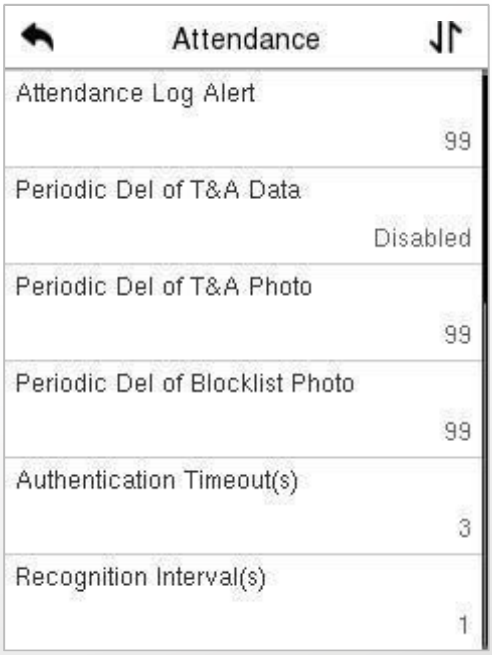
Nota: Por ejemplo, el usuario establece la hora del dispositivo (18:35 del 15 de marzo de 2019) a las 18:30 del 1 de enero de 2020. Después de restaurar la configuración de fábrica, la hora del equipo seguirá siendo las 18:30 del 1 de enero de 2020.

2.2 Configuración de registros de asistencia/acceso

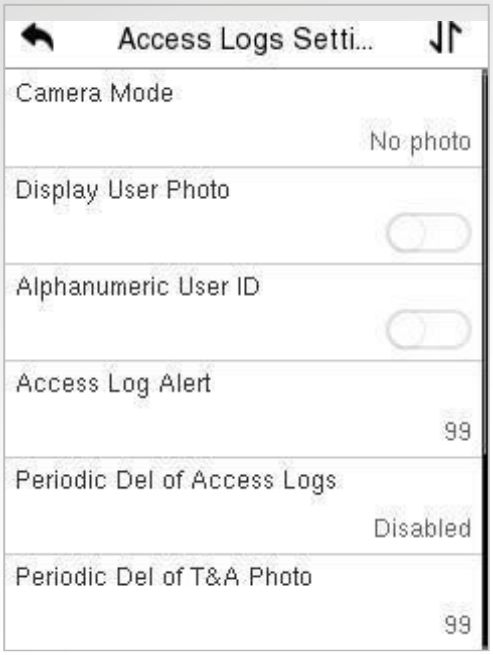
Hacer clic Configuración de registros de asistencia/accesoen la interfaz del sistema.

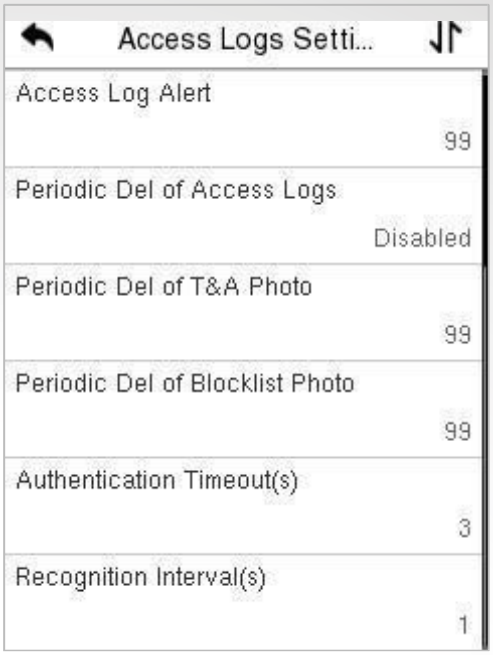
Terminal de control de asistencia:





Nombre de la función	Descripción
Perforadora duplicada Periodo(m)	Dentro de un período de tiempo establecido (unidad: minutos), el registro de asistencia duplicado no se reservará (el valor varía de 1 a 999999 minutos).
Modo cámara	Esta función está desactivada por defecto. Al activarse, aparecerá un aviso de seguridad y el sonido del obturador de la cámara se activará automáticamente. Hay 5 modos: Sin foto: No se tomaron fotografías durante la verificación del usuario. Tomar foto, no guardar: Se toma la foto pero no se guarda durante la verificación. Toma una foto y guárdala:Se toma y se guarda la foto durante la verificación. Guardar en verificación exitosa:Se toma una fotografía y se guarda por cada verificación exitosa. Guardar en verificación fallida:Se tomarán fotografías y se guardarán sólo por cada verificación fallida.
Mostrar foto del usuario	Esta función está deshabilitada por defecto. Al habilitarla, aparecerá un mensaje de seguridad.
ID de usuario alfanumérico	Decide si se admitirán letras en un ID de usuario.
Alerta de registro de asistencia	Cuando el espacio de registro de asistencia alcanza el valor umbral máximo, el dispositivo muestra automáticamente la advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
Envío periódico de T&A Datos	Cuando los registros de asistencia alcanzan su capacidad máxima de almacenamiento, el dispositivo elimina automáticamente un conjunto de registros de asistencia antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.
Envío periódico de T&A Foto	Cuando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Periódico Foto de la lista de bloqueo	Cuando las fotos bloqueadas alcancen su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos bloqueadas antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Autenticación Tiempo(s) de espera	Duración del mensaje de verificación exitosa. Valor válido: 1 a 9 segundos.
Intervalo de reconocimiento (s)	Para configurar el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. Valor válido: 0 a 9 segundos.



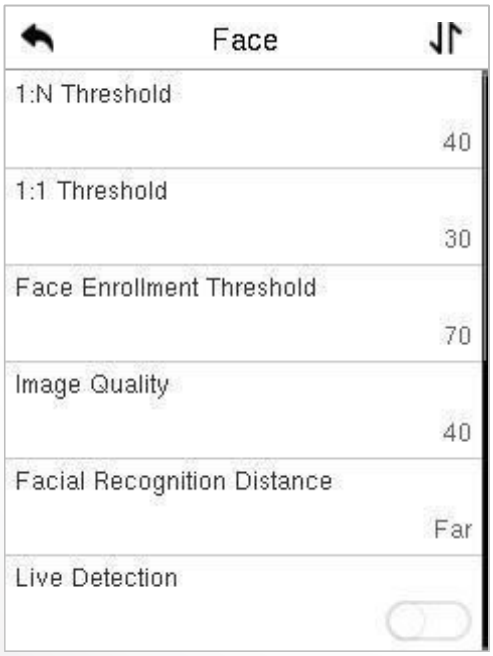


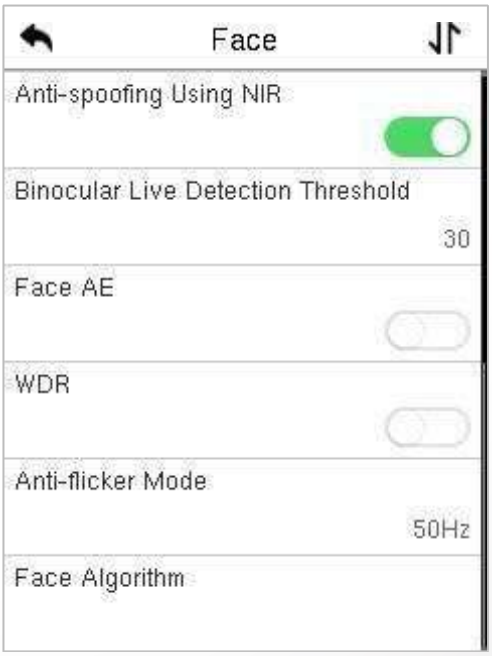
Nombre de la función	Descripción
Modo cámara	Esta función está desactivada por defecto. Al activarse, aparecerá un aviso de seguridad y el sonido del obturador de la cámara se activará automáticamente. Hay 5 modos: Sin foto:No se tomaron fotografías durante la verificación del usuario. Tomar foto, no guardar:Se toma la foto pero no se guarda durante la verificación. Toma una foto y guárdala:Se toma y se guarda la foto durante la verificación. Guardar en verificación exitosa:Se toma y guarda una fotografía para cada verificación exitosa. Guardar en caso de verificación fallida:Se tomará y guardará una foto solo por cada verificación fallida.
Mostrar foto del usuario	Esta función está deshabilitada por defecto. Al habilitarla, aparecerá un mensaje de seguridad.
ID de usuario alfanumérico	Decide si se admitirán letras en un ID de usuario.
Alerta de registro de asistencia	Cuando el espacio de registro del acceso de asistencia alcanza el valor umbral máximo, el dispositivo mostrará automáticamente la advertencia de espacio de memoria. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 9999.
Envío periódico de T&A Datos	Cuando los registros de acceso alcancen su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de registros de acceso antiguos. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 999.

Entrega periódica de T&A Foto	Cuando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos de asistencia antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Periódico Foto de la lista de bloqueo	Cuando las fotos bloqueadas alcancen su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos bloqueadas antiguas. Los usuarios pueden desactivar la función o establecer un valor válido entre 1 y 99.
Autenticación Tiempo(s) de espera	Duración del mensaje de verificación exitosa. Valor válido: 1 a 9 segundos.
Intervalo de reconocimiento (s)	Para configurar el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. Valor válido: 0 a 9 segundos.

6.3 Parámetros de la plantilla de rostro

Toque Face en la interfaz del sistema para ir a los ajustes de parámetro de la plantilla de cara.





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

Nombre de la función	Descripción
Umbral 1:N	En el modo de verificación 1:N, la verificación solo será exitosa cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio y mayor la de rechazo, y viceversa. Se recomienda establecer el valor predeterminado en 75
Umbral 1:1	En el modo de verificación 1:1, la verificación solo será exitosa cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario registradas en el dispositivo sea mayor que el valor establecido. El valor válido oscila entre 0 y 100. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio y mayor la de rechazo, y viceversa. Se recomienda establecer el valor predeterminado en 63.
Inscripción facial Límite	Durante el registro de la plantilla facial, se utiliza una comparación 1:N para determinar si el usuario ya se ha registrado antes. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que este umbral, indica que la plantilla facial ya ha sido registrada.
Calidad de imagen	Calidad de imagen para el registro y la comparación facial. Cuanto mayor sea el valor, mayor será la nitidez de la imagen
Reconocimiento facial Distancia	El reconocimiento de la plantilla facial a la distancia máxima que supere este valor se filtrará. El valor del parámetro indica el tamaño de la plantilla facial necesario para el registro y la comparación. Cuanto mayor sea la distancia a las personas, menores serán los píxeles de la plantilla facial obtenidos por el algoritmo. Si el valor es 0, significa que la distancia de comparación de la plantilla facial es ilimitada.
Detección en vivo	Detecta el intento de suplantación de identidad utilizando imágenes de luz visible para determinar si la muestra fuente biométrica proporcionada es de una persona real (un ser humano vivo) o una representación falsa.
Uso de anti-spoofing NIR	Uso de imágenes de espectros de infrarrojo cercano para identificar y prevenir ataques con fotos y vídeos falsos
Binocular Live Umbral de detección	Es conveniente determinar si las imágenes espectrales del infrarrojo cercano son fotos o videos falsos. Cuanto mayor sea el valor, mejor será la capacidad anti-suplantación de la imagen espectral del infrarrojo cercano.
Cara AE	Cuando el rostro está frente a la cámara en el modo Face AE, el brillo del área del rostro aumenta, mientras que otras áreas se vuelven más oscuras.
Amplio rango dinámico (WDR)	El amplio rango dinámico (WDR) 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 entornos brillantes y oscuros.
Modo antiparpadeo	Se usa cuando el WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea con la misma frecuencia que la luz.
Algoritmo facial	Información relacionada con el algoritmo facial y pausar la actualización de la plantilla facial.

Notas	Un ajuste incorrecto de los parámetros de exposición y calidad puede afectar gravemente el rendimiento del dispositivo. Ajuste la exposición únicamente bajo la supervisión del personal de servicio posventa de nuestra empresa.

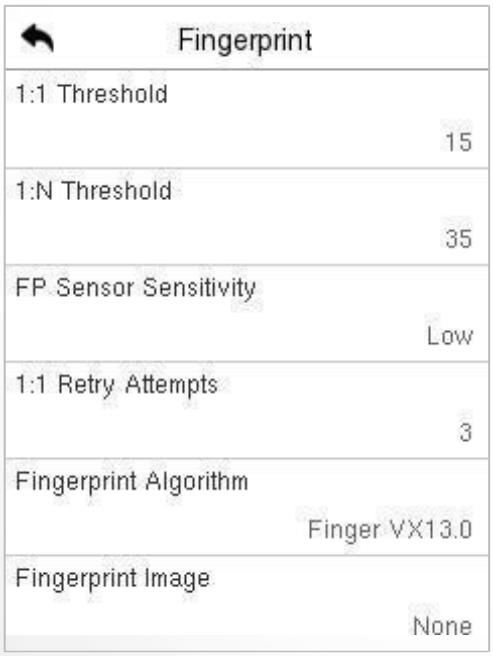
Proceso para modificar la precisión del reconocimiento facial

- En el Sistema interfaz, toque en Rostroy luego alternar para habilitar Anti-spoofing Using NIR para configurar la protección contra la suplantación de identidad.
- Luego, en el Menú principal, grifo Autotest > Prueba facialy realizar la prueba facial.
- Toque tres veces para ver las puntuaciones en la esquina superior derecha de la pantalla y el rectángulo rojo Pulse tres veces para las puntuaciones en la esquina superior derecha de la pantalla, y el cuadro rectangular rojo aparece para comenzar a ajustar el modo.

Mantenga el dispositivo a una distancia de un brazo de su rostro. Se recomienda no moverlo demasiado.

6.4 Parámetros de huellas dactilares

Haga clic en Huella digital en la interfaz del sistema.



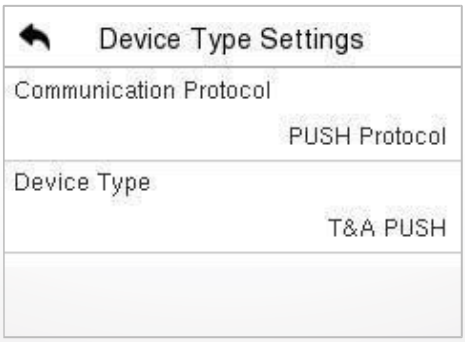
FRR	FRR	Recomendado por coincidencia umbrales	
		1:N	1:1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Bajo	25	10

Nombre de la función	Descripción
Umbral 1:1	En el método de verificación 1:1, la verificación solo será exitosa cuando la similitud entre los datos de huellas dactilares adquiridos y la plantilla de huellas dactilares asociada con el ID de usuario ingresado registrado en el dispositivo sea mayor que el valor establecido.

1: Umbral N	En el método de verificación 1:N, la verificación solo será exitosa cuando la similitud entre los datos de huellas dactilares adquiridos y las plantillas de huellas dactilares registradas en el dispositivo sea mayor que el valor establecido.
Sensor FP Sensibilidad	Para configurar la sensibilidad de la adquisición de huellas dactilares, se recomienda usar el nivel predeterminado.Medio". Cuando el ambiente es seco, lo que resulta en una detección lenta de huellas dactilares, puede establecer el nivel en "Alto"para aumentar la sensibilidad; cuando el ambiente es húmedo, lo que dificulta la identificación de la huella dactilar, puede establecer el nivel en "Bajo".
Reintento 1:1 Intentos	En la verificación 1:1, los usuarios podrían olvidar la huella dactilar registrada o presionarla incorrectamente. Para reducir el proceso de reingreso del ID de usuario, se permite el reintento.
Huella dactilar Algoritmo	Se utiliza para cambiar la versión del algoritmo de huella dactilar. Compatible con ZKFinger VX13.0 por defecto, pero puede cambiarse a ZKFinger VX10.0.
Imagen de huella dactilar	Esta función está deshabilitada por defecto. Tras deshabilitarla, la imagen de la huella dactilar no se mostrará al registrarla ni verificarla. La interfaz del menú permite habilitar o deshabilitar esta función, y aparecen avisos de seguridad al activarla. Hay cuatro opciones disponibles: Mostrar para inscribirse:para mostrar la imagen de la huella digital en la pantalla solo durante el registro. Mostrar para el partido:para mostrar la imagen de la huella digital en la pantalla solo durante la verificación. Mostrar siempre:para mostrar la imagen de la huella digital en la pantalla durante el registro y la verificación. Ninguno:no mostrar la imagen de la huella digital.

6.5 Configuración deltipo de dispositivo

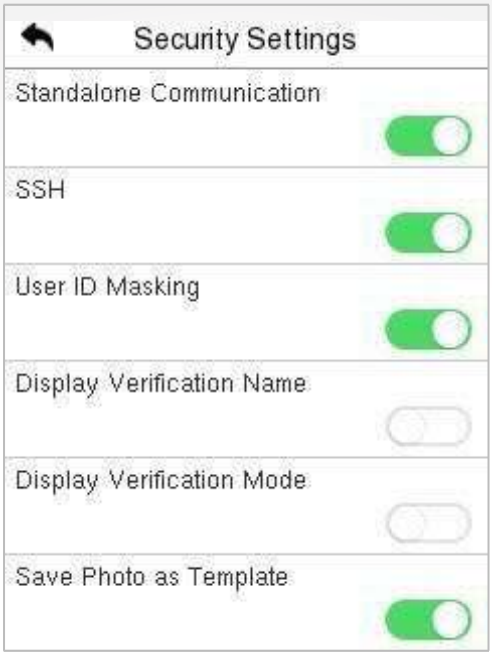
Toque Configuración de tipo de dispositivo en la interfaz del sistema.



Nombre de la función	Descripción
Protocolo de comunicación	Establecer el protocolo de comunicación del dispositivo.
Tipo de dispositivo	Configure el dispositivo como terminal de control de asistencia (T&APUSH) o terminal de control de acceso (A&C PUSH).

6.6 Configuración de seguridad

Configuración de seguridad en el Sistema interfaz.



Nombre de la función	Descripción
Autónomo Comunicación	Esta función está deshabilitada por defecto. Puede habilitarla o deshabilitarla desde el menú. Al activarla, aparecerá un mensaje de seguridad y el dispositivo se reiniciará tras confirmar.
SSH	El dispositivo no es compatible con la función Telnet, por lo que SSH se suele usar para la depuración remota. SSH está habilitado por defecto. La interfaz de menú permite habilitar y deshabilitar SSH. Al habilitarlo, aparecerá un mensaje de seguridad, pero no será necesario reiniciar el dispositivo tras la confirmación.
Enmascaramiento de ID de usuario	Una vez habilitado, el ID de usuario se mostrará parcialmente después del resultado de la verificación de personal (solo el ID de usuario con más de 2 dígitos admite la visualización enmascarada) y está habilitado de manera predeterminada.
Mostrar Nombre de verificación	Una vez habilitada, el nombre del usuario se mostrará después del resultado de la verificación de personal. El resultado de la verificación no mostrará el nombre después de deshabilitarla.
Mostrar Modo de verificación	Una vez activada, la verificación de personal mostrará el modo de verificación del usuario. Si la desactiva, no lo mostrará
Guardar foto como Plantilla	Después de deshabilitar esta función, será necesario volver a registrar la plantilla facial luego de una actualización del algoritmo.

6.7 Actualización USB

Actualización USB en el Sistema interfaz.

El firmware del dispositivo se puede actualizar con el archivo de actualización en una unidad USB. Antes de realizar esta operación, asegúrese de que la unidad USB contenga el archivo de actualización correcto y esté correctamente insertada en el dispositivo.
Si no hay ningún disco USB insertado, el sistema mostrará el siguiente mensaje después de tocarActualización USBen la interfaz del sistema.



Nota: Si necesita un archivo de actualización, póngase en contacto con nuestro soporte técnico. Normalmente, no se recomienda la actualización del firmware.

6.8 Actualizar firmware en línea

Hacer clic Actualizar firmware en líneaen la interfaz del sistema.

Hacer clic Habilitar la actualización de firmware en línea Función, el dispositivo le avisará que la actualización puede traer algunos riesgos de seguridad de datos, lo que requiere confirmación manual por parte del usuario (si la función de configuración de seguridad está desactivada, la advertencia de riesgo no se mostrará cuando la actualización en línea esté activada).



Hacer clic Buscar actualizaciones Puede tener los siguientes 3 escenarios:

- Si la consulta falla, la interfaz indicará "Consulta fallida".
- Si la versión del firmware del dispositivo es la más reciente, indicará que la versión del firmware actual ya es la más reciente.
- Si la versión de firmware del dispositivo no es la más reciente, se mostrará el número de versión y el registro de cambios de la última versión. Los usuarios pueden optar por actualizar a la última versión de firmware.

6.9 Restablecimiento de fábrica

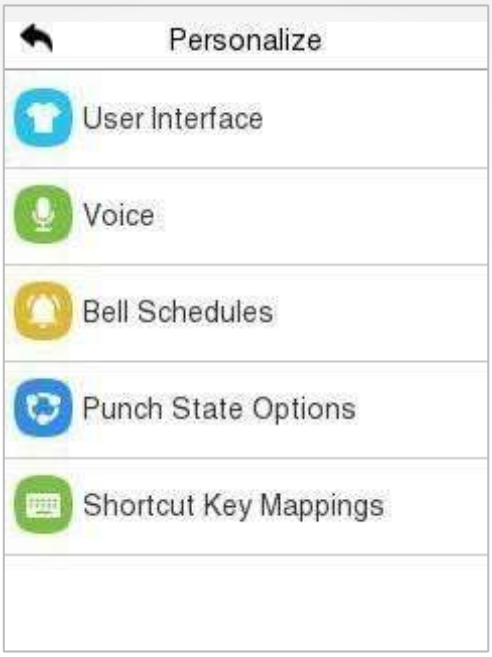
Toque Restablecer en la interfaz del sistema y toque Aceptar para restaurar la configuración predeterminada de fábrica



La función de restablecimiento de fábrica restaura la configuración del dispositivo, como la configuración de comunicación y la configuración del sistema, a la configuración predeterminada de fábrica (esta función no borra los datos del usuario registrado).

7 Personalizar la configuración

Personalizar en elMenú principal Interfaz para personalizar la configuración de la interfaz, opciones de voz, timbre, estado de perforación y asignaciones de teclas de acceso directo.



7.1 Configuración de la interfaz de usuario

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





Nombre de la función	Descripción
Fondo de Pantalla	El fondo de pantalla de la pantalla principal se puede seleccionar según las preferencias del usuario.

Idioma	Seleccione el idioma del dispositivo.
Tiempo de espera del menú (s)	Cuando no se realiza ninguna operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. La función se puede desactivar o establecer el valor requerido entre 60 y 99999 segundos.
Tiempo de inactividad para deslizarse Mostrar(es)	Cuando no se realiza ninguna operación y el tiempo excede el valor establecido, se reproducirá una presentación de diapositivas. Esta función se puede desactivar o se puede configurar entre 3 y 999 segundos.
Intervalo de presentación de diapositivas (s)	Es el intervalo de tiempo para cambiar entre las diferentes fotos de la presentación. Esta función se puede desactivar o configurar entre 3 y 999 segundos.
Tiempo de inactividad hasta el sueño (m)	Si el modo de suspensión está activado y no se realiza ninguna operación en el dispositivo, éste pasará al modo de espera. Toque la pantalla en cualquier lugar para reanudar el funcionamiento normal. Esta función se puede desactivar o configurar con un valor de entre 1 y 999 minutos.
Estilo de pantalla principal	El estilo de la pantalla principal se puede seleccionar según la preferencia del usuario.

7.1 Configuración de voz

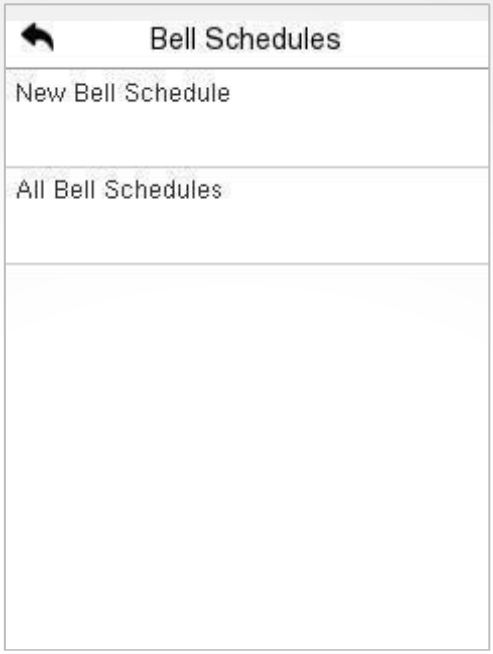
Toque Voz en la interfaz Personalizar para configurar los ajustes de voz



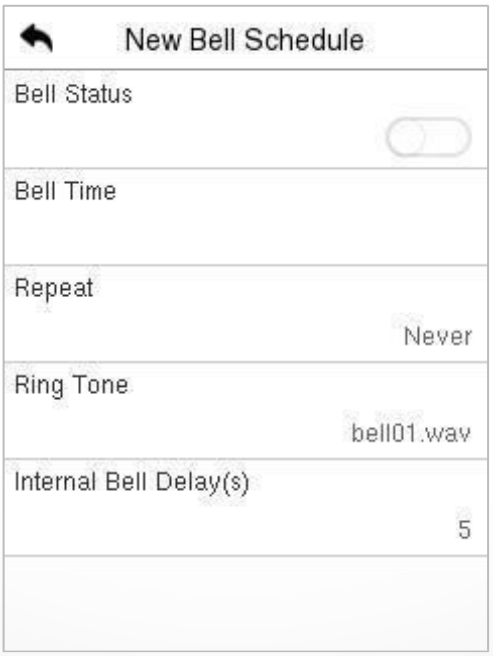
Nombre de la función	Descripción
Aviso de voz	Alterne para habilitar o deshabilitar los mensajes de voz durante las operaciones de la función.
Aviso táctil	Alterne para habilitar o deshabilitar los sonidos del teclado.
Volumen	Ajuste el volumen del dispositivo, que puede configurarse entre 0 y 100.

7.3 Horarios de campana

Horarios de campana en el Personalizar Interfaz para configurar los ajustes de la campana.



Nuevo horario de campanas
Nuevo horario de campanas en la interfaz de programación de campanas para agregar un nuevo horario de campanas



Nombre de la función	Descripción
Estado de la campana	Alterna para habilitar o deshabilitar el estado de la campana.
Hora de campana	Una vez establecido el tiempo requerido, el dispositivo se activará automáticamente para hacer sonar la campana durante ese tiempo.

Repetir	Establezca el número necesario de recuentos para repetir la campana programada.
Tono de llamada	Seleccione un tono de llamada.
Retardo(s) de timbre interno	Establezca el tiempo de repetición de la señal interna. Los valores válidos oscilan entre 1 y 999 segundos.

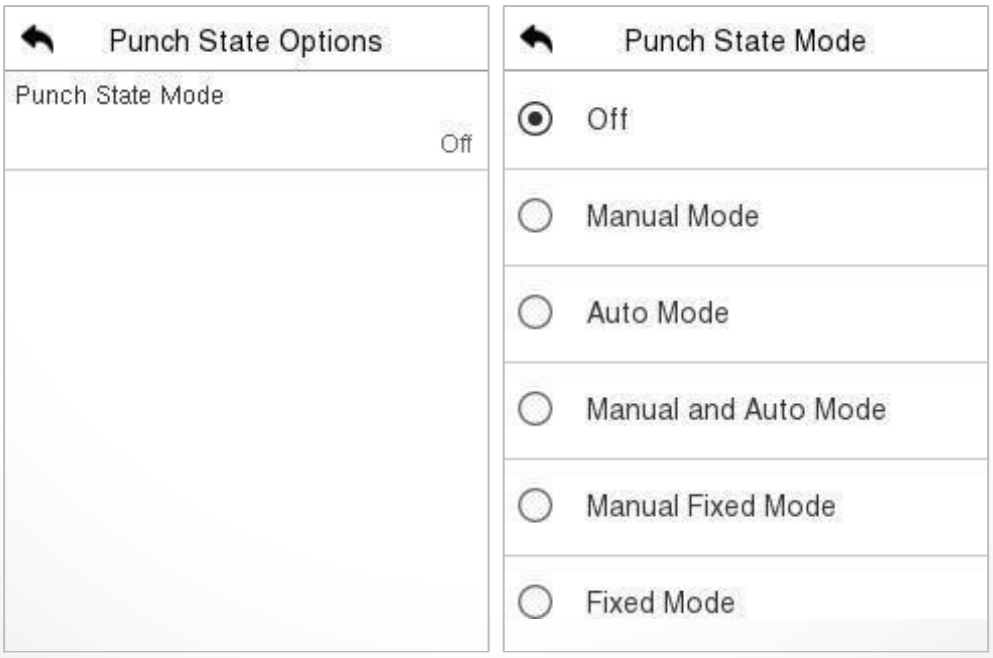
-Horarios de todos los bells:

Una vez programada la campana, en el Horarios de campana interfaz, toque Todos los horarios de campanas- para ver la campana recién programada:
Horario de campanas. El método de edición es el mismo que el de agregar un nuevo horario de campanas.

Edite la campana programada:
En la interfaz de todas las programaciones de campanas, pulse la programación de campanas necesaria, pulse Eliminar y, a continuación, pulse:
Sí para eliminar la campana seleccionada.

7.4 Opciones de estados de punzonado

Toque las opciones de estados de punzonado en la interfaz de personalización para configurar los ajustes del estado de punzonado.



Nombre de la función	Descripción
Modo de estado de golpe	Apagado:Desactivar la función de estado de punzón. Por lo tanto, la clave de estado de punzón configurada en Asignaciones de teclas de acceso directoEl menú dejará de ser válido. Modo manual:Cambie la tecla de estado de perforación manualmente y la tecla de estado de perforación

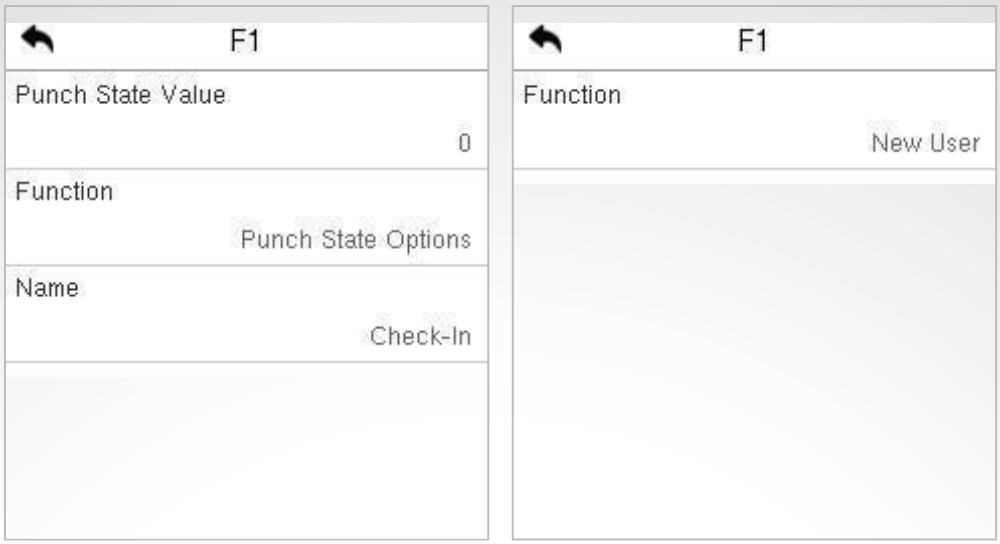
Modo de estado de golpe	desaparecerá después. Tiempo de espera del estado de perforación. Modo automático:La tecla de estado de registro cambiará automáticamente a un estado de registro específico de acuerdo con el cronograma de tiempo predefinido que se puede configurar en las asignaciones de teclas de acceso directo. Modo manual y automático:La interfaz principal mostrará la tecla de cambio automático de estado de fichaje. Sin embargo, los usuarios podrán seleccionar el estado de asistencia manual. Tras el tiempo límite, la tecla de cambio manual de estado de fichaje se convertirá en la tecla de cambio automático de estado de fichaje. Modo fijo manual:Una vez que la tecla de estado de perforación se configura manualmente en un estado de perforación particular, la función permanecerá sin cambios hasta que se cambie manualmente nuevamente. Modo fijo:Solo se mostrará la tecla de estado de fichaje corregida manualmente. Los usuarios no pueden cambiar el estado pulsando ninguna otra tecla.

7.5 Asignaciones de teclas de acceso directo

Los usuarios pueden definir atajos de teclado para el estado de asistencia y las teclas de función, que se definirán en la interfaz principal. De esta manera, al pulsar los atajos de teclado en la interfaz principal, se mostrará directamente el estado de asistencia o la interfaz de función correspondiente.
Asignaciones de teclas de acceso directoen el Personalizar Interfaz para configurar las teclas de acceso directo necesarias.



- En el Asignaciones de teclas de acceso directoInterfaz, toque la tecla de acceso directo requerida para configurar la Configuración de teclas de acceso directo.
- En el Tecla de acceso directo(eso es "F1")interfaz, toquefunciónpara establecer el proceso funcional de la tecla de acceso directo, ya sea una tecla de estado de perforación o una tecla de función.
- Si la tecla de acceso directo está definida como una tecla de función (como Nuevo usuario, Todos los usuarios, etc.), la configuración se completa como se muestra en la imagen a continuación.

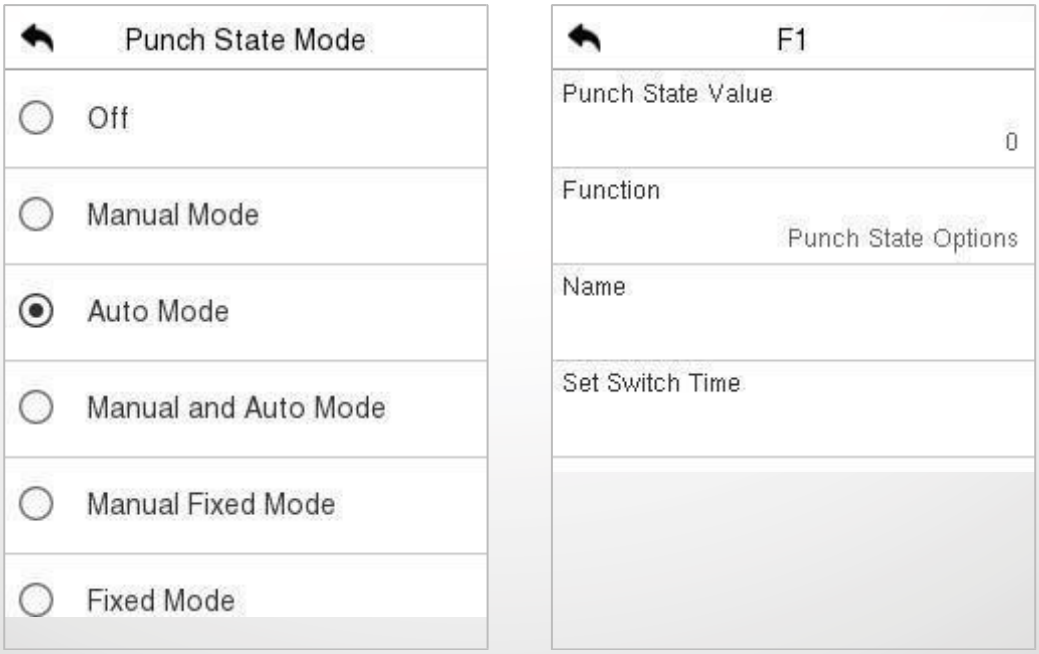


- Si la tecla de acceso directo se configura como una tecla de estado de registro (como registrar entrada, registrar salida, etc.), entonces es necesario configurar el valor de estado de registro (valor válido 0~250), nombre.

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

Establecer la hora del cambio

- El tiempo de cambio se establece de acuerdo con las opciones del estado de perforación.
- En el Opciones de estados de perforacióninterfaz, cuando elmodo de estado de perforaciónestá configurado paramodo automático, se debe establecer el tiempo de conmutación.
- En el Tecla de acceso directointerfaz, toqueEstablecer hora de cambiopara establecer la hora del cambio.
- En el Ciclo de conmutaciónInterfaz, seleccione el ciclo de conmutación (lunes, martes, etc.) como se muestra en la imagen a continuación.
- Una vez seleccionado el ciclo de cambio, configure la hora de cambio para cada día y toque DE ACUERDO para confirmar, como se muestra en la imagen de abajo.




Switch Cycle
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

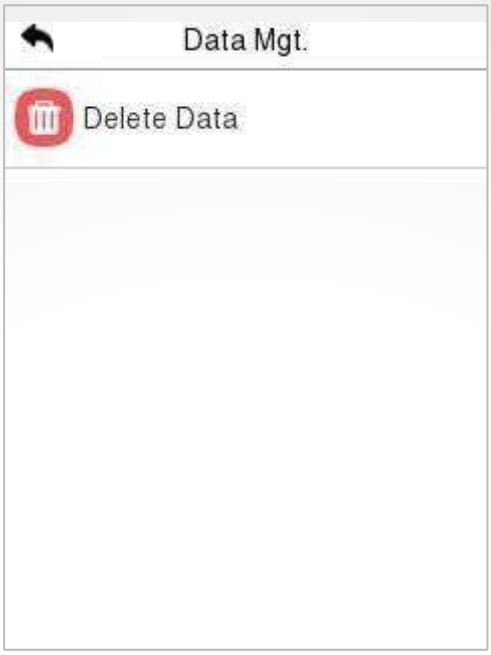

Set Switch Time
Switch Cycle
Daily
Monday
Tuesday
Wednesday
Thursday
Friday


Monday
12:00
12
00
HH
MM
Confirm (OK)
Cancel (ESC)


Set Switch Time
Switch Cycle
Daily
Monday
12:00
Tuesday
Wednesday
Thursday
Friday

8 Gestión de datos

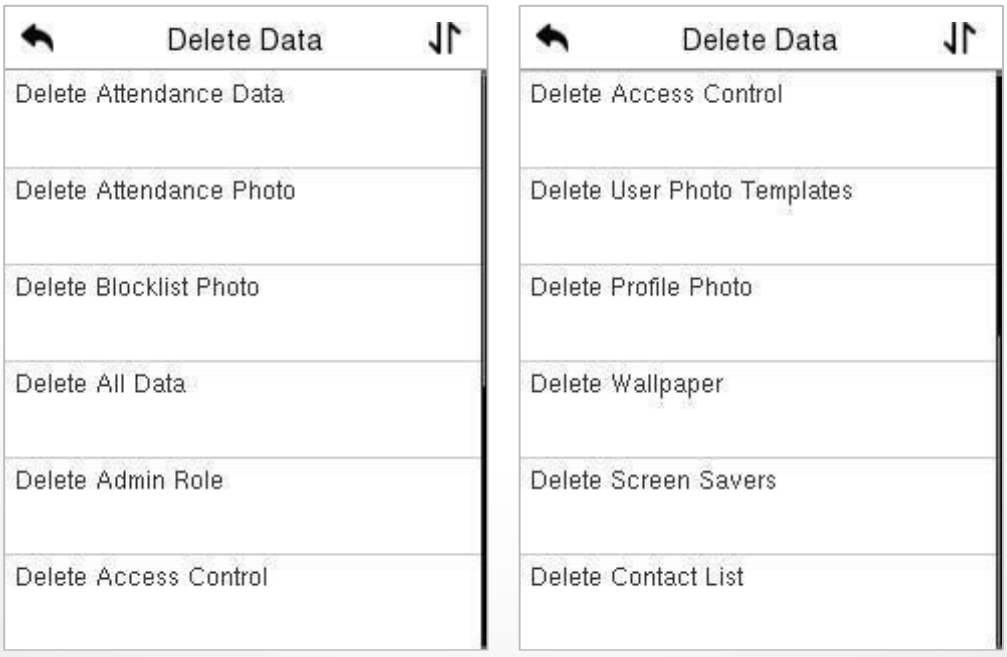
En el Menú principal, Gestión de datos para borrar los datos relevantes en el dispositivo.



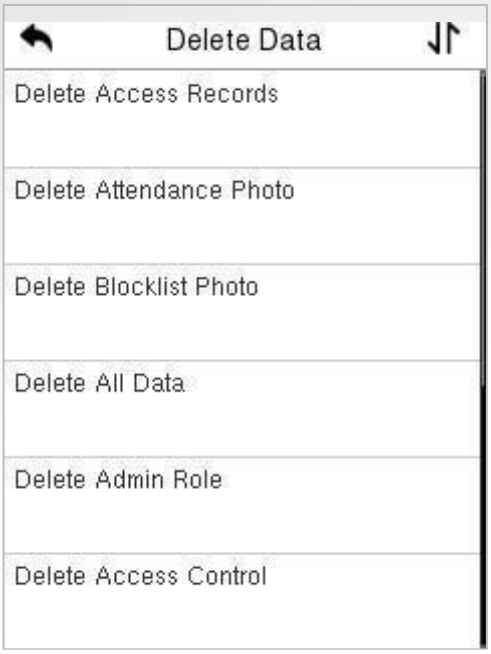
8.1 Eliminar datos

Eliminar datos en el Gestión de datos Interfaz para eliminar los datos requeridos.

Terminal de control de asistencia:



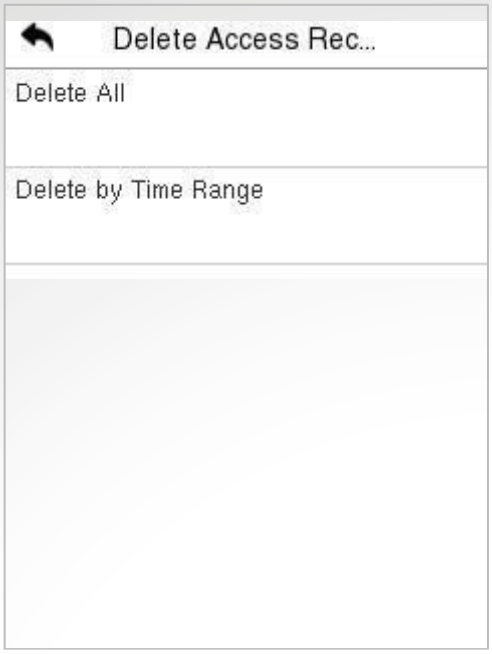
Terminal de control de acceso:





Nombre de la función	Descripción
Eliminar datos de asistencia /Eliminar registros de acceso	Para eliminar datos de asistencia/registros de acceso de forma condicional.
Eliminar foto de asistencia	Para eliminar fotos de asistencia del personal designado.
Eliminar foto de la lista de bloqueo	Para eliminar las fotos tomadas durante verificaciones fallidas.
Eliminar todos los datos	Para eliminar información y registros de asistencia/registros de acceso de todos los usuarios registrados.
Eliminar rol de administrador	Para eliminar todos los privilegios de administrador.
Eliminar el control de acceso	Para eliminar todos los datos de acceso.
Eliminar foto de usuario Plantillas	Para eliminar las plantillas de fotos de usuario en el dispositivo. Al eliminar las fotos de plantilla, hay un recordatorio de riesgo: "Es necesario volver a registrar el rostro después de una actualización del algoritmo."
Eliminar foto de perfil	Para eliminar todas las fotos de usuario en el dispositivo.
Eliminar fondo de pantalla	Para eliminar todos los fondos de pantalla del dispositivo.
Eliminar protectores de pantalla	Para eliminar los protectores de pantalla en el dispositivo.
Eliminar lista de contactos	Para eliminar toda la lista de contactos del videoportero en el dispositivo.

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



Seleccionar Eliminar por rango de tiempo.

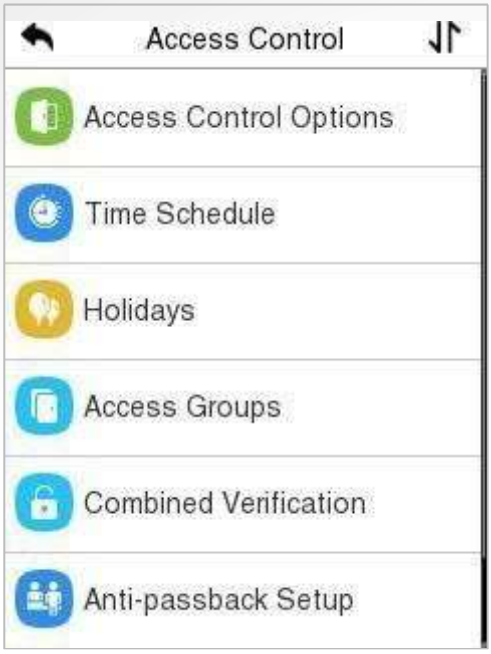


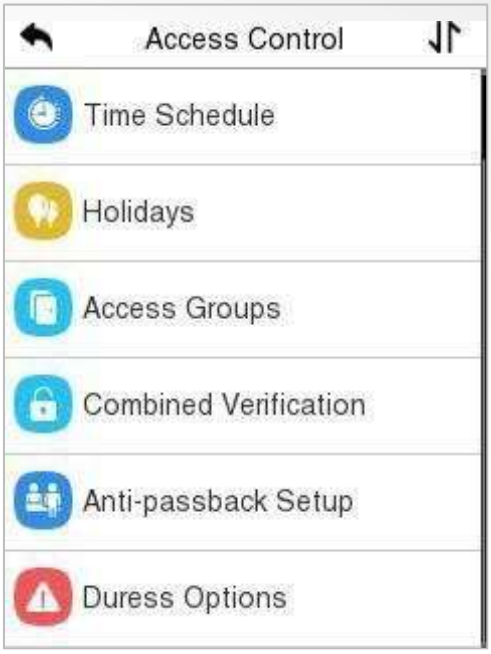
Establezca el rango de tiempo y haga clic DE ACUERDO.

9 Control de acceso

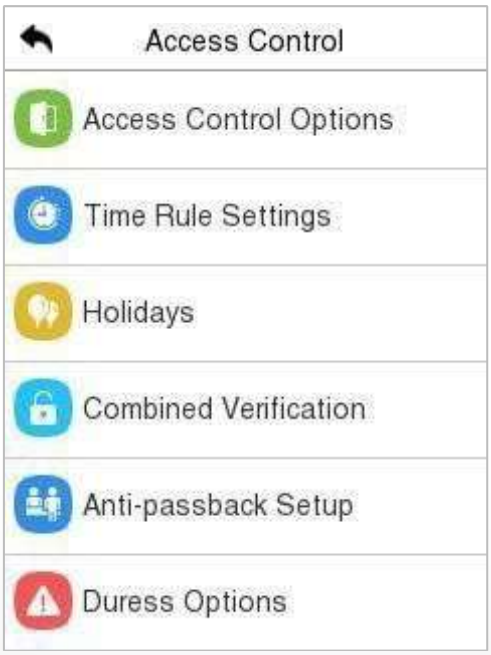
En el Menú principal, Control de acceso para establecer el horario de apertura de puertas, control de cerraduras y configurar otros parámetros relacionados con el control de acceso.

Terminal de control de asistencia:





Terminal de control de asistencia:



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

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

- El grupo de usuario correspondiente debe estar ya configurado en la combinación de desbloqueo de la puerta (y si hay otros grupos configurados en la misma combinación de acceso, entonces también se requiere la verificación de los miembros de esos grupos para desbloquear la puerta).

- En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria del grupo predeterminada, donde el combo de acceso es "1" y está configurado en estado de desbloqueo de manera predeterminada.

9.1 Opciones de control de acceso

Opciones de control de accesoen el Control de acceso Interfaz para configurar los parámetros del bloqueo de control del terminal y equipos relacionados.

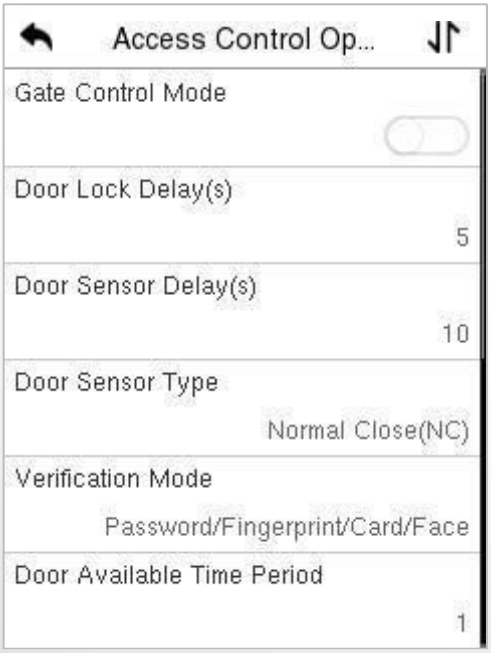
Terminal de control de asistencia:

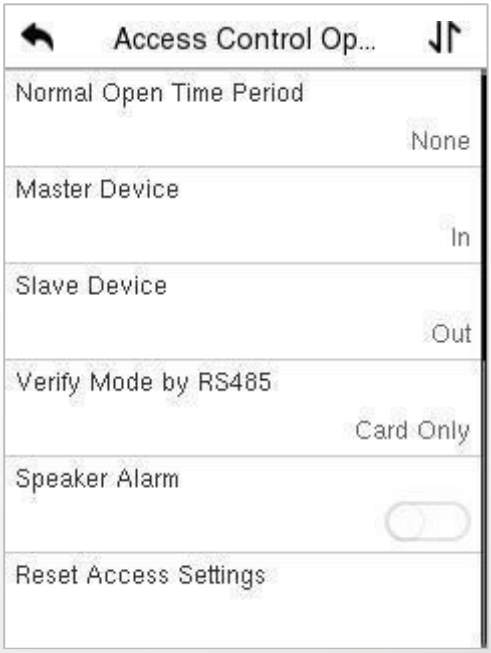


Nombre de la función	Descripción
Retardo (s) de bloqueo de puerta	El tiempo que el dispositivo controla el desbloqueo de la cerradura eléctrica. Valor válido: 1 a 10 segundos; 0 segundos indica la desactivación de la función.
Sensor de puerta Retraso(s)	Si la puerta no está bloqueada y se deja abierta durante un tiempo determinado (retardo del sensor de puerta), se activará una alarma. El valor válido de DoorSensorDelay varía entre 1 y 255 segundos.
Tipo de sensor de puerta	Hay tres tipos de sensores:Ninguno, Normal AbiertoyNormal Cerrado. Ninguno: Significa que el sensor de la puerta no está en uso. Normal abierto:Significa que la puerta siempre se deja abierta cuando hay energía eléctrica encendida. Normal Cerrado:Significa que la puerta siempre permanece cerrada cuando hay energía eléctrica encendida.
Alarma de puerta Retraso(s)	Cuando el estado del sensor de la puerta es inconsistente con el del tipo de sensor de la puerta, se activará la alarma después de un período de tiempo; este período de tiempo es el Retardo de alarma de puerta (el valor varía de 1 a 999 segundos).

Reintentar veces a Alarma	Cuando el número de verificaciones fallidas alcance el valor establecido (el valor varía de 1 a 9), se activará la alarma. Si el valor establecido es Ninguno, la alarma no se activará tras una verificación fallida.
Cierre normal Periodo de tiempo	Es el período de tiempo programado para el modo "Cierre normal" para que la puerta esté siempre cerrada durante este período.
Normal abierto Periodo de tiempo	Periodo de tiempo programado para el modo "Normalmente Abierto", de modo que la puerta siempre permanezca abierta durante este periodo.
Entrada auxiliar Configuración	Establece el tiempo de desbloqueo de la puerta y el tipo de salida auxiliar del dispositivo terminal auxiliar. Los tipos de salida auxiliar incluyen: Ninguna, Activar apertura de puerta, Activar alarma, Activar apertura de puerta y Alarma.
Verificar modo por RS485	El modo de verificación se utiliza cuando el dispositivo funciona como host o esclavo. Los modos de verificación compatibles incluyen Solo Tarjeta y Tarjeta + Contraseña.
Días festivos válidos	Para establecer si Período de tiempo de cierre normal o Período de tiempo abierto normal. La configuración es válida durante el período de vacaciones establecido. Seleccione [EN] para habilitar el conjunto o NO período de tiempo en vacaciones.
Alarma de altavoz	Transmite una alarma sonora o de desmontaje desde el local. Cuando la puerta se cierra o la verificación es exitosa, el sistema cancela la alarma desde el local.
Restablecer acceso Ajustes	Los parámetros de restablecimiento del control de acceso incluyen el retardo de bloqueo de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el tiempo de disponibilidad de la puerta, el tiempo de apertura normal, el dispositivo maestro y la alarma. Sin embargo, se excluyen los datos de control de acceso borrados en la Gestión de Datos.

Terminal de control de asistencia:





Nombre de la función	Descripción
Puerta Control viejo Modo	Alterne entre el interruptor ON o OFF para entrar en el modo de control de puerta o no. Cuando se establece enEN, en esta interfaz, se eliminarán las opciones Relé de bloqueo de puerta, Relé de sensor de puerta y Tipo de sensor de puerta.
Cerradura de puerta Demora (s)	El tiempo que el dispositivo controla el desbloqueo de la cerradura eléctrica. Valor válido: 1 a 10 segundos; 0 segundos indica la desactivación de la función.
Puerta Sensor o Delay (s)	Si la puerta no está bloqueada y se deja abierta durante un período determinado (retardo del sensor de puerta), se activará una alarma. El valor válido de DoorSensorDelay varía entre 1 y 255 segundos.
Sensor de puerta Tipo	Hay tres tipos de sensores:Ninguno, Normal AbiertoyNormal Cerrado.Ninguno:Significa que el sensor de la puerta no está en uso. Normal abierto:Significa que la puerta siempre se deja abierta cuando hay energía eléctrica encendida. Normal Cerrado:Significa que la puerta siempre permanece cerrada cuando hay energía eléctrica encendida.
Verificación Modo	El modo de verificación admitido incluye Contraseña/Huella dactilar/Tarjeta/Rostro, Solo huella dactilar, Solo ID de usuario, Contraseña, Solo tarjeta, Huella dactilar/Contraseña, Huella dactilar/Tarjeta, ID de usuario + Huella dactilar, Huella dactilar + Contraseña, Huella dactilar + Tarjeta, Huella dactilar + Contraseña + Tarjeta, Contraseña + Tarjeta, Contraseña/Tarjeta, ID de usuario + Huella dactilar + Contraseña, Huella dactilar + (Tarjeta/ID de usuario), Solo rostro, Rostro + Huella dactilar, Rostro + Contraseña, Rostro + Tarjeta, Rostro + Huella dactilar + Tarjeta y Rostro + Huella dactilar + Contraseña.
Puerta Disponible Tiempo Período	Para establecer el período de tiempo para la puerta, de modo que la puerta esté disponible solo durante ese período.
Normal Abierto Tiempo Período	Periodo de tiempo programado para el modo "Normalmente Abierto", de modo que la puerta siempre permanezca abierta durante este periodo.
Dispositivo maestro	Al configurar el maestro, el estado del maestro se puede configurar para salir al ingresar. Afuera: El registro verificado en el host es el registro de salida. En:El registro verificado en el host es el registro de entrada.
Dispositivo esclavo	Al configurar el esclavo, el estado del esclavo se puede configurar para que salga al ingresar. Afuera:El registro verificado en el host es el registro de salida. En:El registro verificado en el host es el registro de entrada.
Verificar Modo por RS485	El modo de verificación se utiliza cuando el dispositivo funciona como host o esclavo. Los modos de verificación compatibles incluyen Solo Tarjeta y Tarjeta + Contraseña.
Alarma de altavoz	Transmite una alarma sonora o de desmontaje desde el local. Cuando la puerta se cierra o la verificación es exitosa, el sistema cancela la alarma desde el local.
Reiniciar Acceso Configuración	Los parámetros de restablecimiento del control de acceso incluyen el retardo de bloqueo de la puerta, el retardo del sensor de la puerta, el tipo de sensor de la puerta, el modo de verificación, el tiempo de disponibilidad de la puerta, el tiempo de apertura normal, el dispositivo maestro y la alarma. Sin embargo, se excluyen los datos de control de acceso borrados en la Gestión de Datos.

9.2 Configuración de reglas de tiempo/programación horaria

Configuración de la programación horaria/reglas de tiempoen la interfaz de Control de Acceso para configurar los ajustes de tiempo.

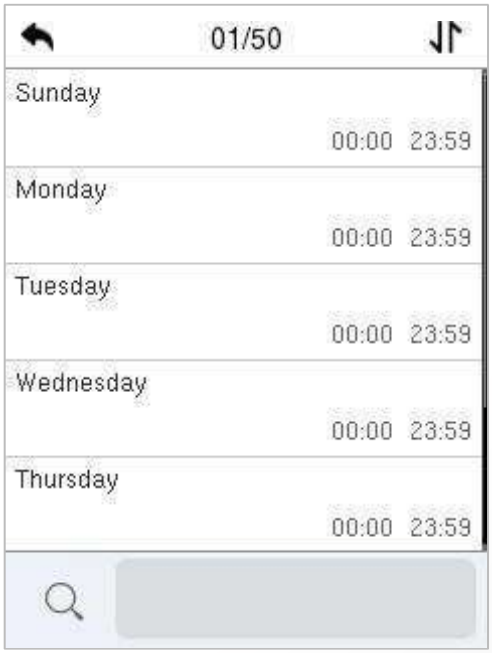
- El sistema completo puede definir hasta 50 períodos de tiempo.
- Cada período de tiempo representa 10 Zonas horarias, es decir 1 semana y 3 días festivos, y cada zona horaria es un período estándar de 24 horas por día y el usuario solo puede verificar dentro del período de tiempo válido.
- Se puede establecer un máximo de tres períodos de tiempo para cada zona horaria. La relación entre estos períodos es "O". Por lo tanto, cuando el momento de la verificación cae en cualquiera de estos períodos de tiempo, la verificación es válida.
- El formato de zona horaria de cada período de tiempo: HH MM-HH MM, que es preciso en minutos según el reloj de 24 horas.

Utilice el cuadro gris para buscar la zona horaria requerida y especifique el número de zona horaria requerida (máximo: hasta 50 zonas).

Terminal de asistencia:



Terminal de control de asistencia:



En la interfaz de número de zona horaria seleccionada, pulse el día requerido (es decir, lunes, martes, etc.) para establecer la hora.



Especifique la hora de inicio y la hora de finalización y luego toque DE ACUERDO.

Notas:

- Cuando la hora de finalización es anterior a la hora de inicio (por ejemplo, 23:57~23:56), indica que el acceso está prohibido durante todo el día.
- Cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 00:00~23:59), indica que el intervalo es válido.
- El período de tiempo efectivo para mantener la puerta desbloqueada o abierta todo el día es (00:00~23:59) o también cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 08:00~23:59).
- La zona horaria predeterminada 1 indica que la puerta está abierta todo el día.

9.3 Vacaciones

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

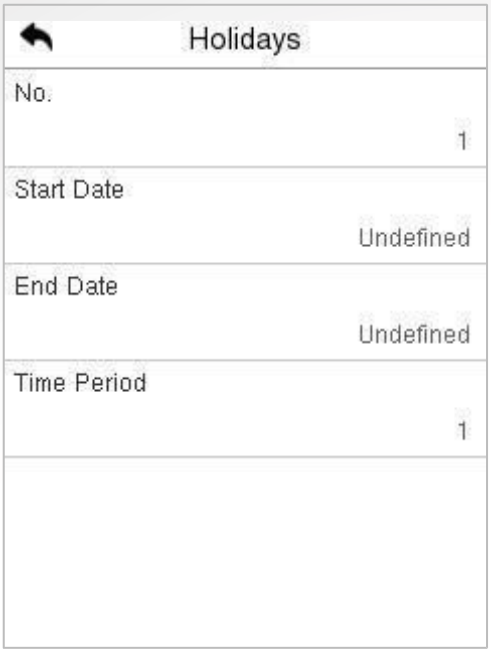
Vacaciones en el Control de acceso Interfaz para configurar el acceso de vacaciones.



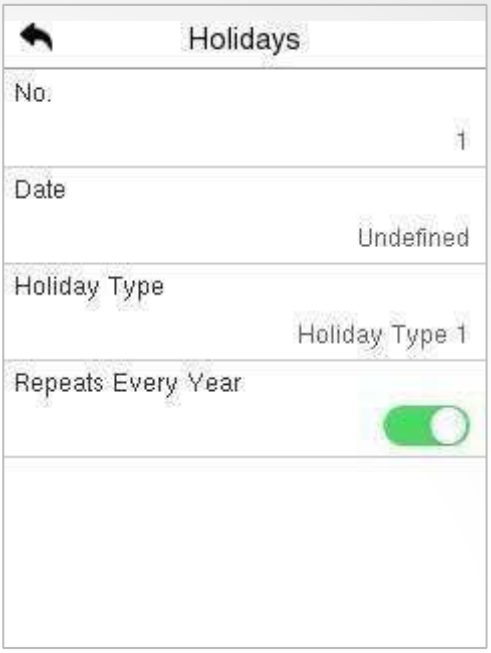
Añadir un nuevo día festivo:

Añadir vacacionesen el Vacaciones Interfaz y configure los parámetros de vacaciones.

Terminal de control de asistencia:



Terminal de control de acceso:



Editar un día festivo:

En el VacacionesInterfaz, seleccione un elemento de vacaciones para modificar. ToqueEditarpara modificar los parámetros de vacaciones.

Eliminar un día festivo:

En el Vacaciones Interfaz, seleccione un elemento de vacaciones que desee eliminar y toque Borrar. Presiona DE ACUERDO Para confirmar la eliminación. Después de la eliminación, estas vacaciones ya no se muestran en Todas las vacaciones interfaz.

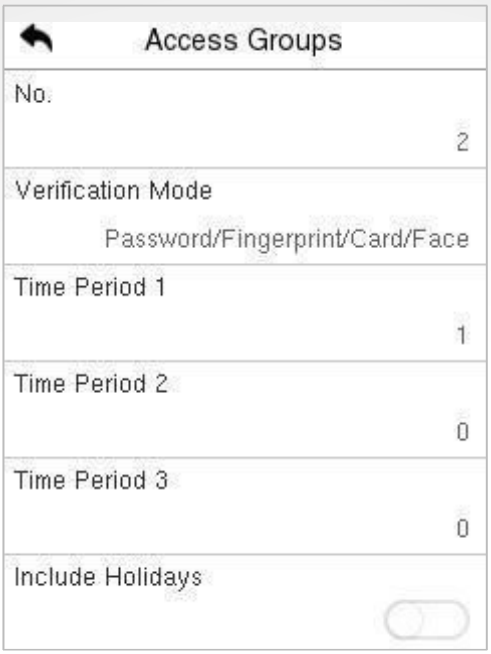
9.4 Grupos de acceso

Esto facilita la gestión de grupos y usuarios en diferentes grupos de acceso. La configuración de un grupo de acceso, como las zonas horarias, se aplica a todos los miembros del grupo de forma predeterminada. Sin embargo, los usuarios pueden configurar las zonas horarias manualmente según sea necesario. La autenticación de usuarios prevalece sobre la autenticación de grupo cuando los modos de autenticación de grupo se solapan con los métodos de autenticación individuales. Cada grupo puede establecer un máximo de tres zonas horarias. De forma predeterminada, los usuarios recién registrados se asignan al Grupo de Acceso 1; pueden asignarse a otros grupos de acceso.
Hacer clic Grupos de acceso en el Control de acceso interfaz.



Agregar un nuevo grupo

Hacer clic Nuevo grupo en la interfaz de Grupos de acceso y configure los parámetros del grupo de acceso.



Notas:

- Esta función solo se utiliza con el sistema de asistencia push (T&A PUSH).
- Hay un grupo de acceso predeterminado numerado 1, que no se puede eliminar, pero sí se puede modificar.
- Un número no se puede modificar después de haberlo establecido.
- Cuando se establece que el feriado sea válido, el personal de un grupo solo podrá abrir la puerta cuando la zona horaria del grupo se superponga con el período de feriado.
- Cuando las vacaciones se establecen como inválidas, el tiempo de control de acceso del personal de un grupo no se ve afectado durante las vacaciones.

9.5 Verificación combinada

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

Verificación combinada en elControl de acceso Interfaz para configurar la configuración de verificación combinada



En la interfaz de verificación combinada, toque la combinación de desbloqueo de puerta que desea configurar y toque el arriba y abajo para ingresar el número de combinación y luego presione DE ACUERDO.
Ejemplo:

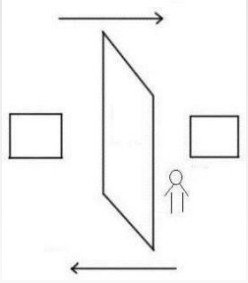
- El Combinación de desbloqueo de puerta 1se establece como(01 03 05 06 08), indicando que la combinación de desbloqueo 1 consta de 5 personas, y los 5 individuos son de 5 grupos, a saber,Grupo de control de acceso1 (grupo AC 1), grupo AC 3, grupo AC 5, grupo AC 6 y grupo AC 8, respectivamente.
- El Combinación de desbloqueo de puerta 2se establece como(02 02 04 04 07), lo que indica que la combinación de desbloqueo 2 consta de 5 personas; las dos primeras son del grupo AC 2, las dos siguientes son del grupo AC 4 y la última persona es del grupo AC 7.
- El Combinación de desbloqueo de puerta 3se establece como(09 09 09 09 09), lo que indica que hay 5 personas en esta combinación; todas ellas del grupo AC 9.
- El Combinación de desbloqueo de puerta 4se establece como(03 05 08 00 00), lo que indica que la combinación de desbloqueo 4 consta de solo tres personas: la primera persona pertenece al grupo AC 3, la segunda al grupo AC 5 y la tercera al grupo AC 8.

Eliminar una combinación para desbloquear una puerta:

Establezca todas las combinaciones de desbloqueo de puertas en 0 si desea eliminar las combinaciones de desbloqueo de puertas.

9.6 Configuración anti-passback

Es posible que personas sigan a los usuarios para entrar sin verificación, lo que podría provocar una brecha de seguridad. Para evitar esta situación, se desarrolló la opción Anti-Passback. Una vez activada, el registro de entrada debe coincidir con el de salida para poder abrir la puerta.
Esta función requiere que dos dispositivos funcionen juntos: uno se instala dentro de la puerta (dispositivo maestro) y el otro se instala fuera de la puerta (dispositivo esclavo). Los dos dispositivos se comunican a través de Señal Wiegand. El formato Wiegand y el tipo de salida (ID de usuario/Número de tarjeta) adoptados por el dispositivo maestro y el dispositivo esclavo deben ser consistentes.



Configuración anti-passbacken el Control de acceso interfaz.

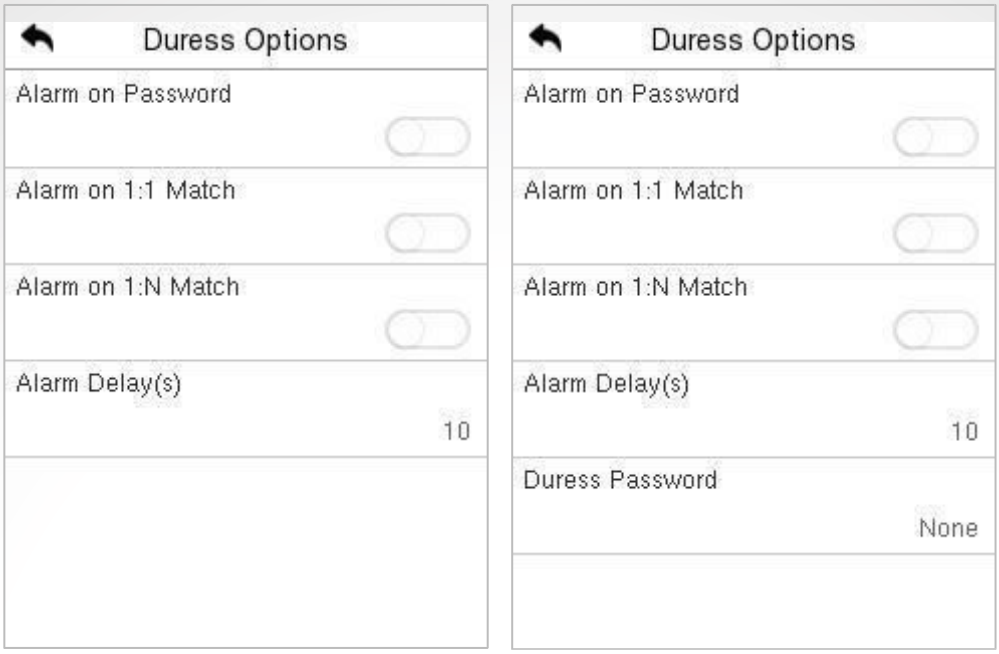


Nombre de la función	Descripción
Anti-passback Dirección	Sin anti-passback:La función anti-passback está deshabilitada, lo que significa que la verificación exitosa, ya sea mediante el dispositivo maestro o el dispositivo esclavo, puede desbloquear la puerta. El estado de asistencia no se guarda en esta opción. Salida Anti-passback:Tras el check-out, solo si el último registro corresponde a un check-in, el usuario podrá volver a salir; de lo contrario, se activará la alarma. Sin embargo, el usuario podrá realizar el check-in libremente. En Anti-passback:Después de que un usuario registre su entrada, solo si el último registro es de salida, podrá volver a registrarla; de lo contrario, se activará la alarma. Sin embargo, podrá registrar su salida libremente. Anti-passback de entrada/salida:Después de que un usuario realiza el check-in/check-out, solo si el último registro es un registro de check-out, el usuario puede realizar el check-in nuevamente; o si es un registro de check-in, el usuario puede realizar el check-out nuevamente; de lo contrario, se activará la alarma.

9.7 Opciones de coacción

Una vez que un usuario activa la función de verificación de coacción con métodos de autenticación específicos, y cuando está bajo coacción y se autentica utilizando la verificación de coacción, el dispositivo desbloqueará la puerta como de costumbre, pero al mismo tiempo, se enviará una señal para activar la alarma.

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



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

10 Administrador USB

Puede importar la información del usuario y los datos de asistencia de la máquina al software de asistencia correspondiente para procesarlos mediante un disco USB, o importar la información del usuario a otros dispositivos para realizar copias de seguridad.

Antes de cargar o descargar datos desde o hacia el disco USB, inserte primero el disco USB en la ranura USB.

Nota: Solo se admite el formato FAT32 al descargar datos mediante un disco USB.

Administrador de USBen la interfaz del menú principal.

Terminal de control de asistencia:



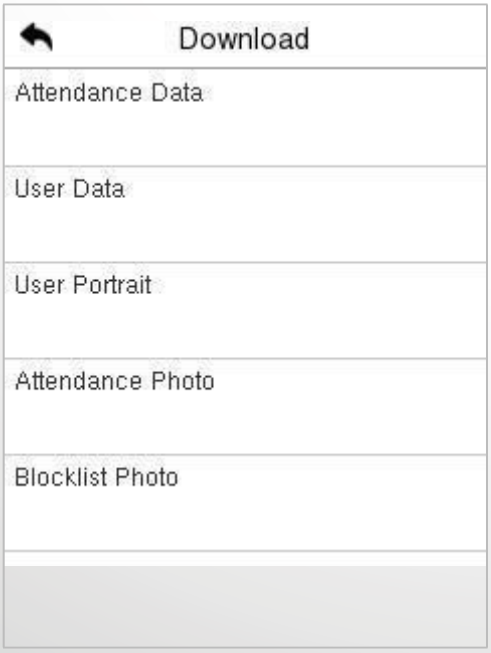
Terminal de control de acceso:



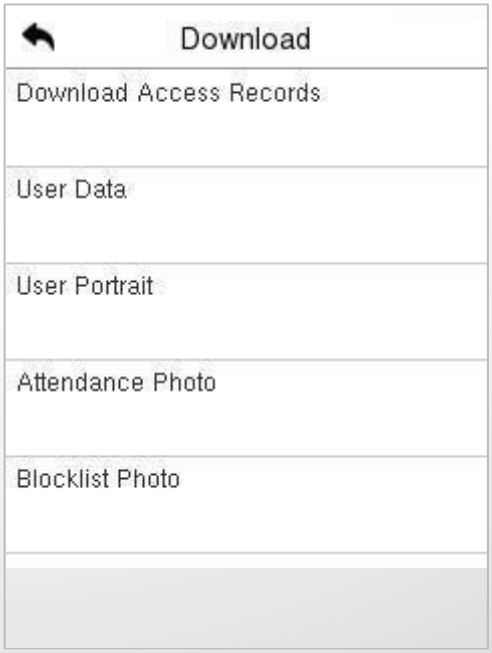
10.1 Descarga USB

En el Administrador USB interfaz, toque Descargar.

Terminal de control de asistencia:



Terminal de control de acceso:



Nombre de la función	Descripción
Datos de asistencia /Acceso a descargas	Para descargar todos los datos de asistencia/registros de acceso en un período de tiempo especificado en un disco USB.
Datos del usuario	Para descargar toda la información del usuario del dispositivo al disco USB.
Retrato de usuario	Para descargar todos los retratos de usuario del dispositivo al disco USB.
Foto de asistencia	Para descargar todas las fotos de asistencia desde el dispositivo al disco USB.
Foto de la lista de bloqueo	Para descargar todas las fotos bloqueadas (fotos tomadas después de verificaciones fallidas) del dispositivo al disco USB.

10.2 Carga USB

En la interfaz de USB Manager, toque Descargar.

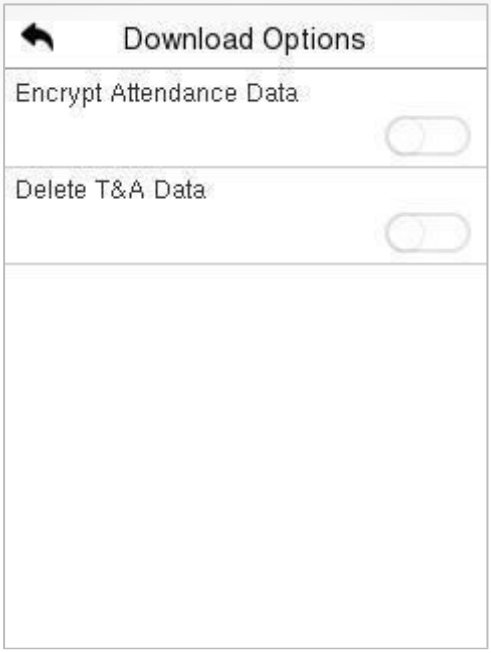


Nombre de la función	Descripción
Protector de pantalla	Para cargar todos los protectores de pantalla desde la memoria USB al dispositivo, puede elegir "Subir la foto seleccionada" o "Subir todas las fotos". Las imágenes se mostrarán en la interfaz principal del dispositivo después de la carga.
Papel pintado	Para subir todos los fondos de pantalla desde una memoria USB al dispositivo, puedes elegir "Subir la foto seleccionada" o "Subir todas las fotos". Las imágenes se mostrarán en pantalla después de la subida.
Datos del usuario	Para cargar toda la información del usuario desde el disco USB al dispositivo.
Retrato de usuario	Para cargar todos los retratos de usuario desde el disco USB al dispositivo.

10.3 Opciones de descarga

En el Administrador USB interfaz, toque Opciones de descarga.

Nota:Esta función es solo para terminal de control de asistencia.



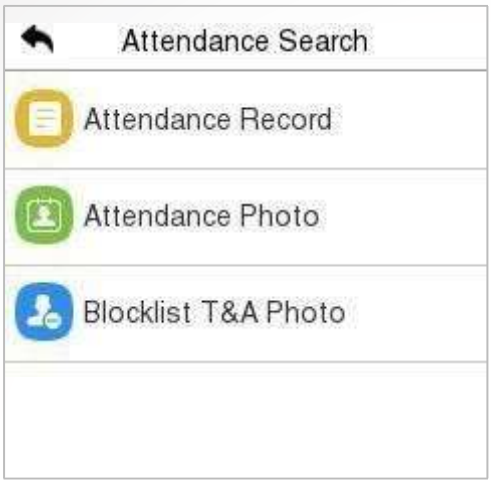
Nombre de la función	Descripción
Protector de pantalla	Los datos de asistencia se cifran durante la carga y descarga.
Eliminar datos de T&A	Después de una descarga exitosa, se eliminan los datos de asistencia del dispositivo.

11 Búsqueda de asistencia

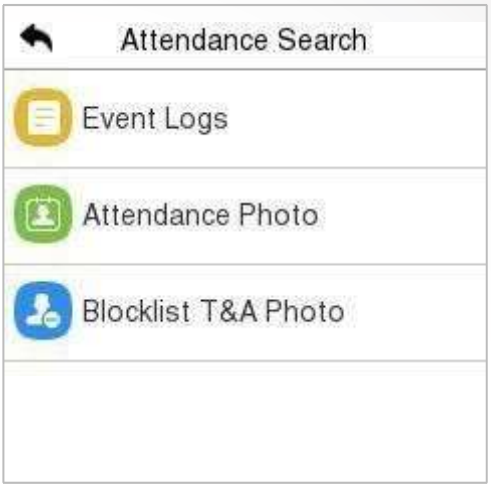
Una vez verificada la identidad de un usuario, los registros de eventos se guardarán en el dispositivo. Esta función permite a los usuarios consultar sus registros de acceso.

Hacer clicBúsqueda de asistenciaen elMenú principalInterfaz para buscar el registro de acceso/asistencia requerido.

Terminal de control de asistencia:



Terminal de control de acceso:



El proceso de búsqueda de fotos de asistencia y de lista negra es similar al de los registros de eventos. A continuación, se muestra un ejemplo de búsqueda de registros de eventos.
En el Búsqueda de asistencia interfaz, toque Registro de asistencia/Registros de eventos para buscar el registro requerido.

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



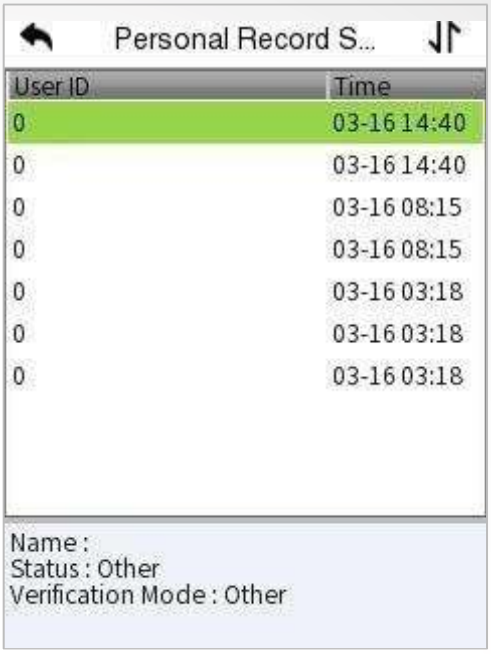
2. Seleccione el rango de tiempo en el que se deben buscar los registros.



3.Una vez que la búsqueda de registros se complete correctamente, toque el inicio de sesión resaltado en verde para ver sus detalles.

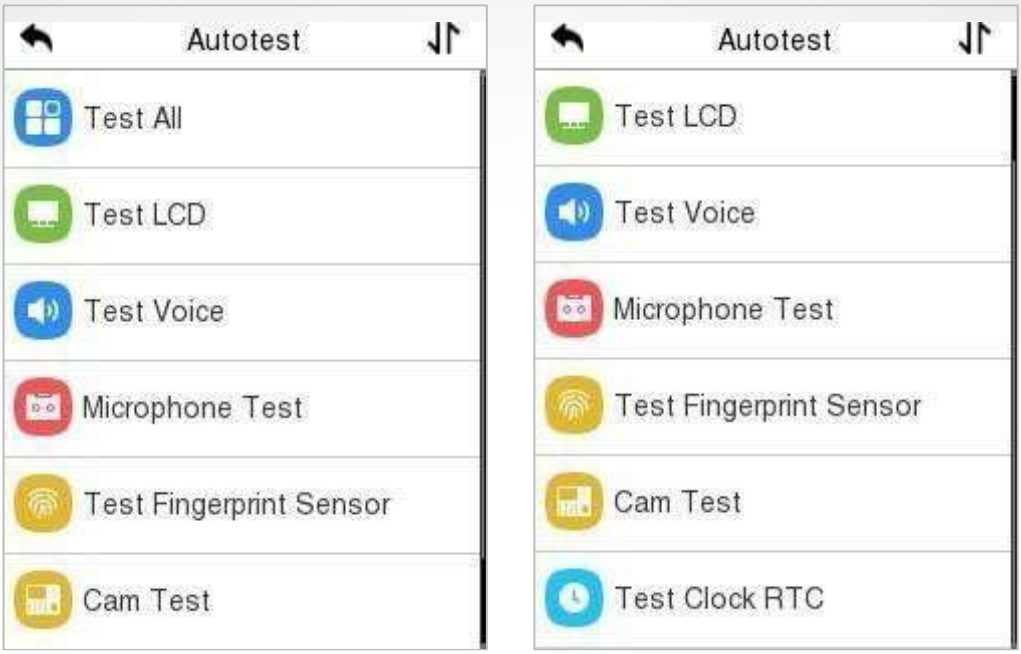


4.La siguiente figura muestra los detalles del registro seleccionado.



12 Autoprueba

En el Menú principal, Autoprueba para probar automáticamente si todos los módulos del dispositivo funcionan correctamente, incluidos la pantalla LCD, la voz, la cámara y el reloj en tiempo real (RTC).



Nombre de la función	Descripción
Probar todo	Para probar automáticamente si la pantalla LCD, el audio, la cámara y el RTC están normales.
Prueba de LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando todo color, blanco puro y negro puro para verificar si la pantalla muestra los colores normalmente.
Voz de prueba	Para probar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de la voz es buena.
Prueba de micrófono	Compruebe si el micrófono funciona hablando al micrófono y reproduciendo la grabación del micrófono.
Prueba de huella dactilar Sensor	Para probar el sensor de huellas dactilares, presione el escáner con el dedo para comprobar si la imagen es nítida. Al presionar el escáner, la imagen se mostrará en la pantalla.
Prueba de leva	Para comprobar si la cámara funciona correctamente, revise las fotos tomadas para ver si son lo suficientemente nítidas. Igual que...Prueba de cara".
Reloj de prueba RTC	Para probar el RTC, el dispositivo comprueba si el reloj funciona con normalidad y precisión con un cronómetro. Toque la pantalla para iniciar el conteo y vuelva a presionarla para detenerlo.

13 Información del sistema

En el Menú principal, Información del sistema para ver el estado de almacenamiento, la información de la versión del dispositivo y la información del firmware.



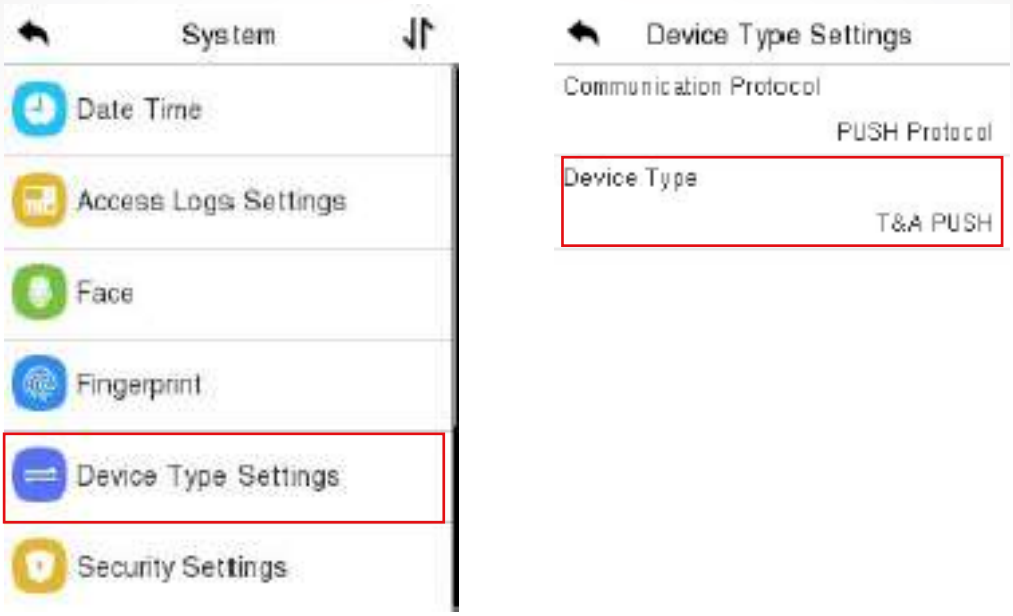
Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento del usuario del dispositivo actual, la contra-seña, la plantilla facial, el almacenamiento de huellas dactilares y tarjetas, los registros de acceso, las fotos de asistencia y de lista de bloqueo, y las fotos de perfil.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC y el algoritmo de huellas dactilares.★, Algoritmo de plantilla facial, informa-ción de la plataforma, versión de MCU y fecha de fabricación.
Información del firmwar	Muestra la versión del firmware y otra información de la versión del dispositivo.
Política de privacidad	El control de la política de privacidad aparecerá al encender el dispositivo por primera vez. Después de hacer clic en "Lo he leído", el cliente puede utilizar el producto con regularidad. Haga clic Información del sistema > Política de privacidadPara ver el contenido de la política de privacidad, no se permite la exportación de Udisc. Nota:El texto de la política de privacidad actual solo está disponible en chino simplificado e inglés. Sin embargo, se está traduciendo contenido multilingüe, con más versiones.

14 Conéctese al software BioTime Cloud

14.1 Agregar dispositivo en el software

1. COMISIÓN.>Ethernet en el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo.

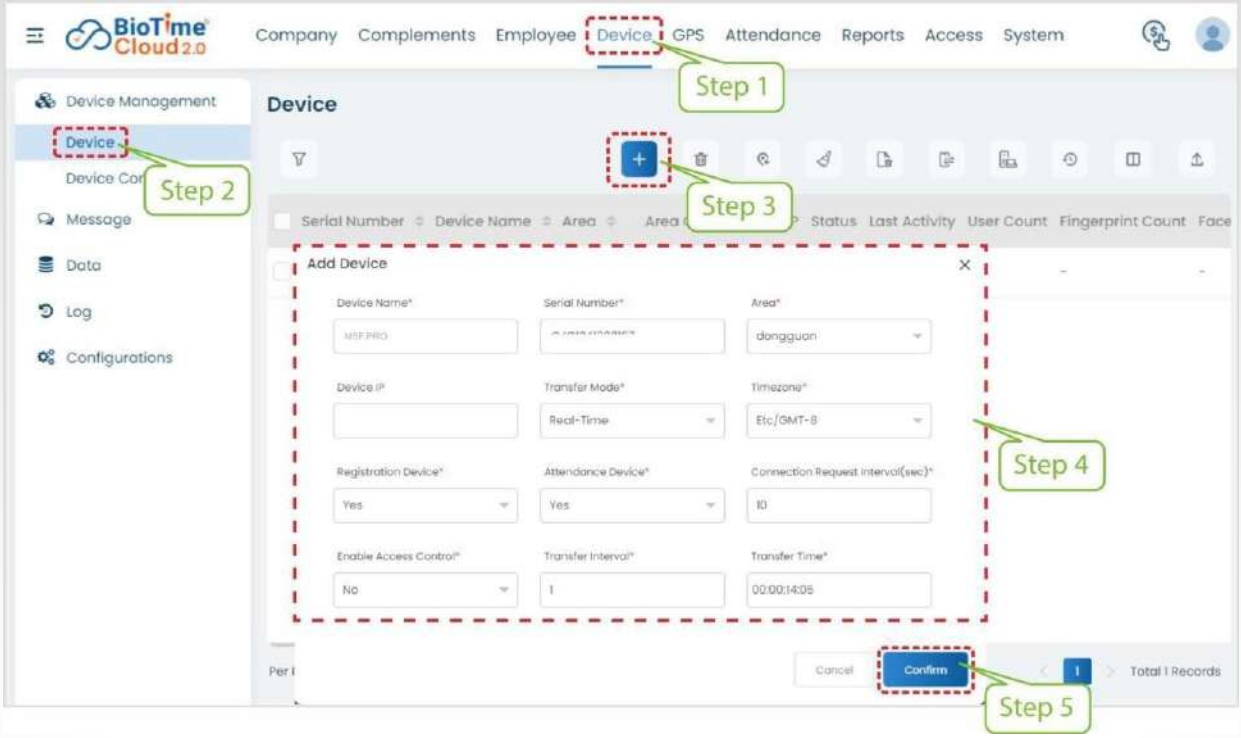
2. Sistema>Configuración del tipo de dispositivo>Tipo de dispositivopara ver y asegurarse de que el tipo de dispositivo esté configurado en T&A PUSH.



3. En el menú principal, haga clic en COMISIÓN.>Configuración del servidor en la nubepara habilitar el nombre de dominio e ingresar el nombre de dominio correcto.

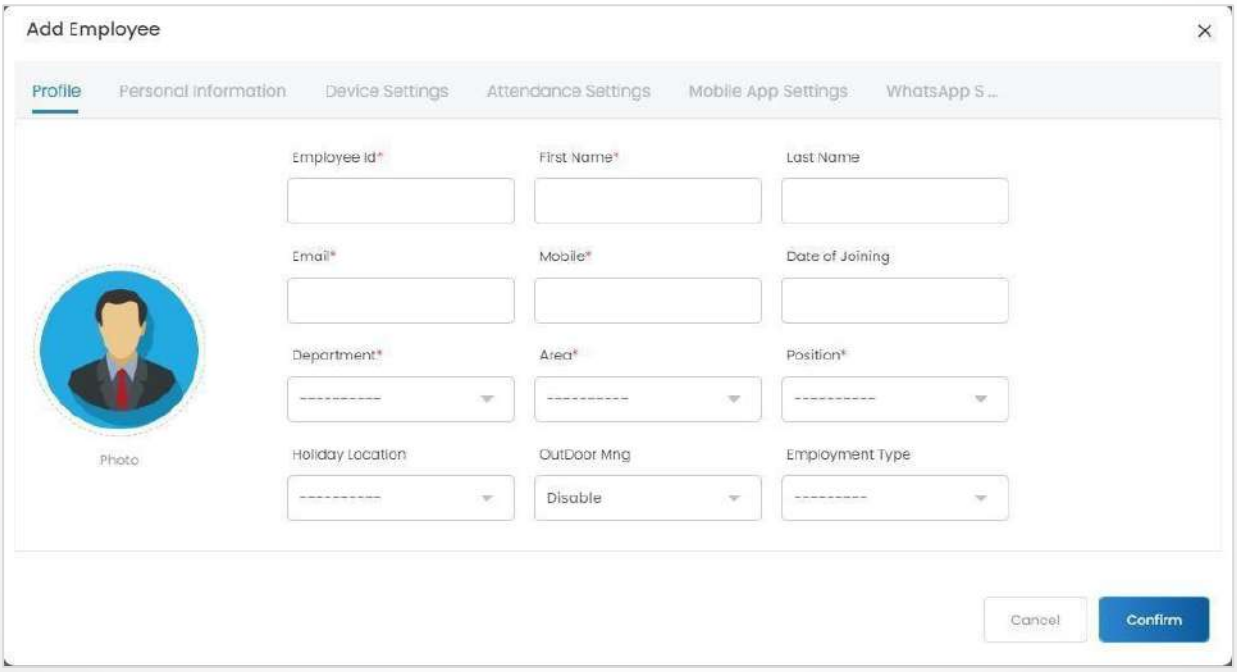


Abra BioTime Cloud y en la interfaz del dispositivo, haga clic en para agregar el dispositivo recién montado al software.



14.2 Agregar personal al software

1. Hacer clic Empleado > Perfil > Empleado >y rellene todos los campos obligatorios para registrar nuevos usuarios en el software.



2. Complete todos los campos obligatorios y haga clic Confirmar para registrar un nuevo usuario.

3. Hacer clicEmpleado > Perfil > Empleado > Resincronizar con dispositivospara sincronizar todos los datos en el dispositivo incluidos los nuevos usuarios.

15 Conéctese al software ZKBio CVAccess

15.1 Establecer la dirección de comunicación

Lado del dispositivo

1. COMISIÓN.>Etherneten el menú principal para configurar la dirección IP y la puerta de enlace del dispositivo.

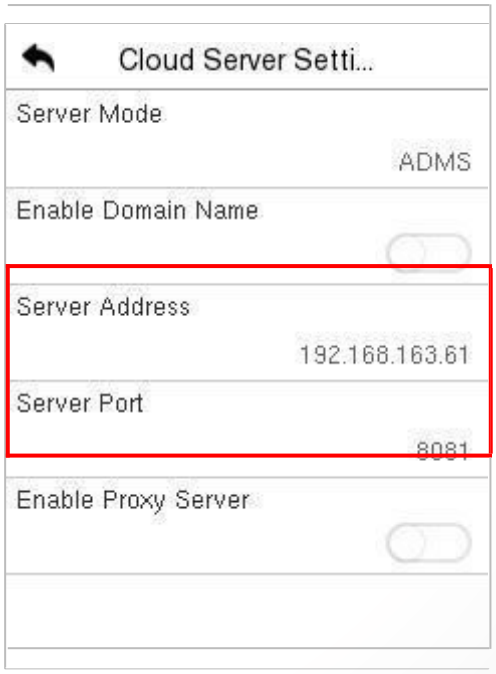
Nota:Asegúrese de que la dirección IP esté en el mismo segmento de red que la dirección del servidor y pueda comunicarse con el servidor ZKBio CVAccess.

2. En el menú principal, haga clic en COMISIÓN.>Configuración del servidor en la nubepara configurar la dirección del servidor y el puerto del servidor.

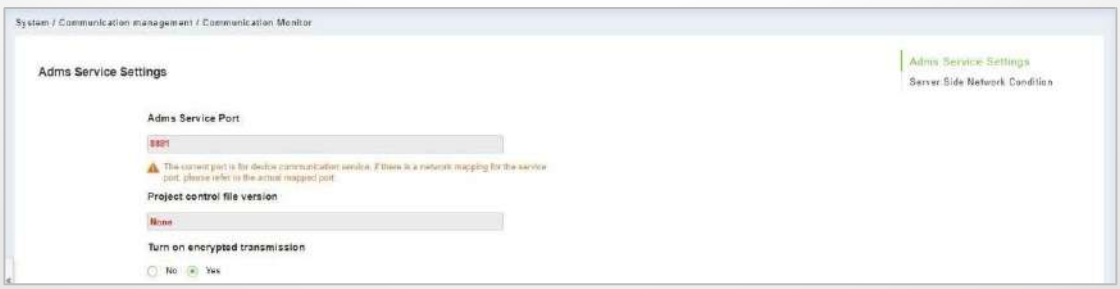
Dirección del servidor: Establecer la dirección IP como de ZKBio CVAccess server.
Puerto del servidor: Establecer el puerto del servidor como de ZKBio CVAccess

Lado del software





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



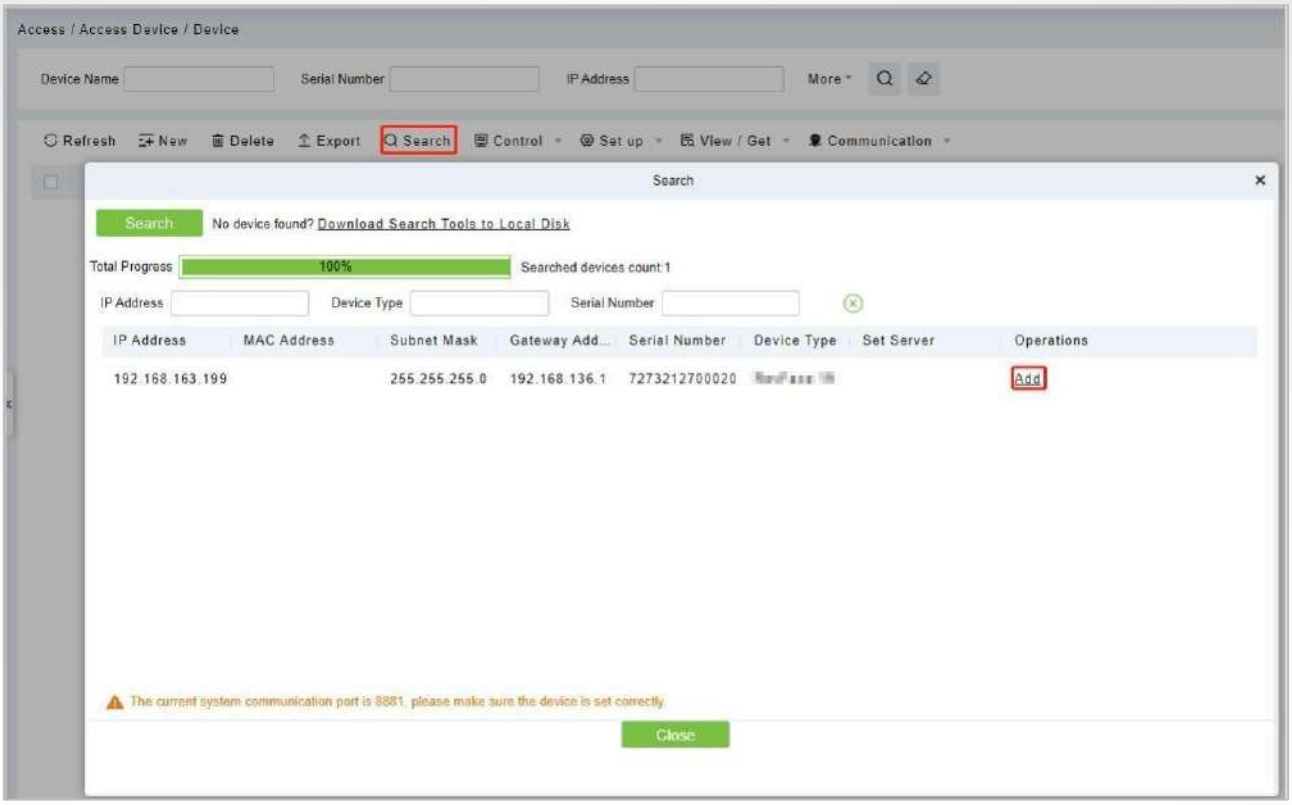
15.2 Agregar dispositivo en el software

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

1.Hacer clicAcceso>Dispositivo>Dispositivo de búsqueda, para abrir la interfaz de búsqueda en el software.

2.Hacer clic Buscar, y te pedirá que lo hagas. Búsqueda…….

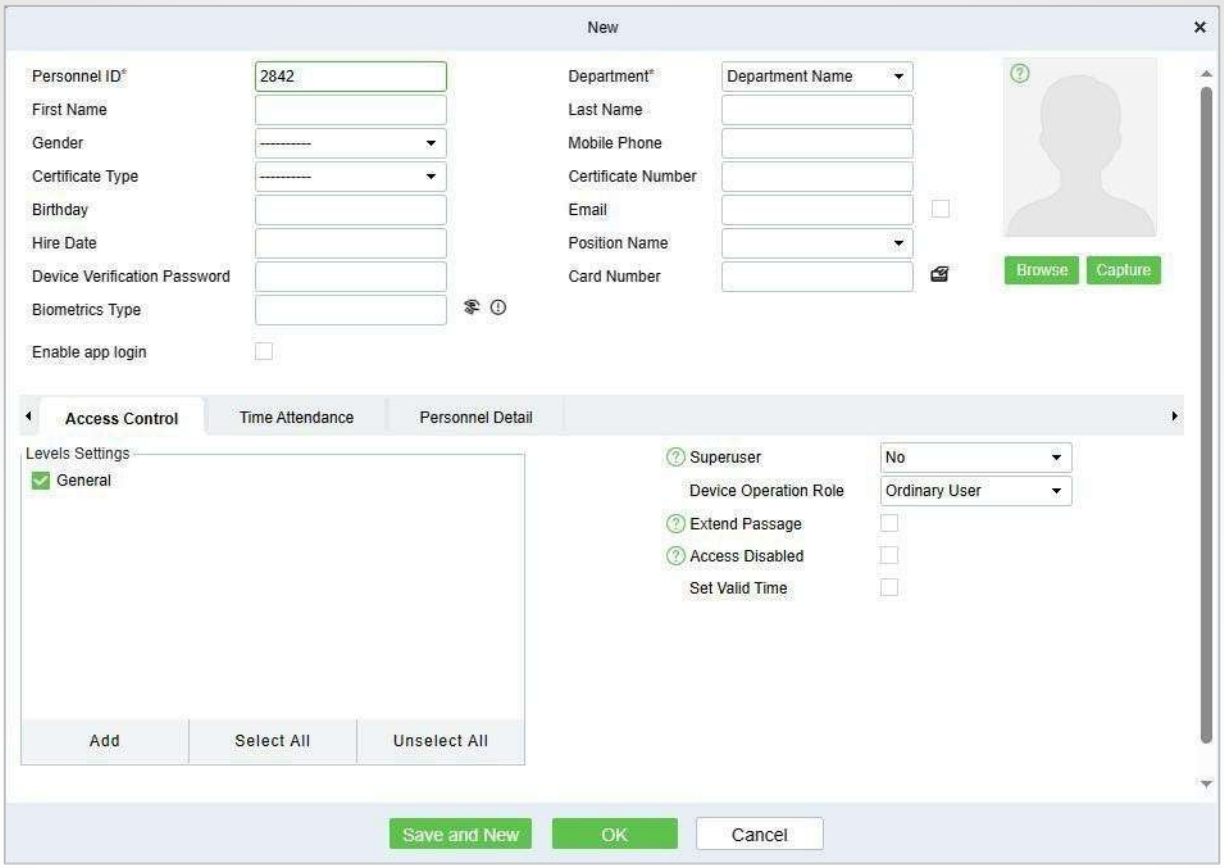
3.Después de la búsqueda, se mostrará la lista y el número total de controladores de acceso.



4. Hacer clicAgregarEn la columna de operación, aparecerá una nueva ventana. Seleccione "Tipo de icono", "Área" y "Añadir a nivel" en cada menú desplegable y haga clic en DE ACUERDO para agregar el dispositivo.

15.3 Agregar personal al software

1. Hacer clicPersonal>Persona>Nuevo:



2. Complete todos los campos obligatorios y haga clic DE ACUERDOpara registrar un nuevo usuario.

3. Hacer clic Acceso > Dispositivo > Control > Sincronizar todos los datos con los dispositivospara sincronizar todos los datos del dispositivo incluidos los nuevos usuarios.

Apéndice 1

Requisitos de Recolección en Vivo y Registro de Plantillas de caras con Visible Light

1. Se recomienda realizar el registro en un ambiente interior con una iluminación adecuada. fuente sin subexposición ni sobreexposición.
2. No coloque el dispositivo cerca de fuentes de luz exteriores, como puertas o ventanas, u otras fuentes de luz intensa.
3. Se recomienda utilizar prendas de color oscuro, diferente al color de fondo para el registro.4
4. Exponga la plantilla de su rostro y su frente correctamente y no cubra la plantilla de su rostro y cejas con tu cabello.
5. Se recomienda mostrar una expresión facial sencilla. (Una sonrisa es aceptable, pero no cierre los ojos ni incline la cabeza).
6. Se requieren dos plantillas para una persona con anteojos, una plantilla con anteojos y la otra sin anteojos.
7. No use accesorios como bufanda o mascarilla que puedan cubrirle la boca o el mentón.
8. Coloque la plantilla directamente hacia el dispositivo de captura y ubique su plantilla de rostro en el área de captura de plantillas como se muestra en la plantilla a continuación.
9. No incluya más de una plantilla de rostro en el área de captura.
10. Se recomienda una distancia de 50 a 80 cm para capturar la plantilla (distancia ajustable según la altura).



Requisitos para los datos de plantillas de rostros digitales de Visible Light

La foto digital debe tener bordes rectos, ser a color, mostrar solo a una persona, quien debe estar sin cartografía y con ropa informal. Quienes usen gafas deben seguir usándolas para la foto.

- Distancia de los ojos

Se recomiendan 200 píxeles o más con una distancia no inferior a 115 píxeles.

- Expresión facial

Se recomienda una plantilla de rostro neutral o una sonrisa con los ojos naturalmente abiertos.

- Gesto y ángel

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 mascarillas ni gafas de colores. La montura de las gafas no debe cubrir los ojos ni reflejar la luz. Para personas con monturas gruesas, se recomienda tomar dos plantillas: una con gafas y otra sin ellas.

- Plantilla de cara

Plantilla de rostro completa con contorno claro, escala real, luz distribuida uniformemente y sin sombras.

- Formato de plantilla

Debe ser BMP, JPG o JPEG.

- Requerimiento de datos

Debe cumplir con los siguientes requisitos:

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

Apéndice 2

Política de privacidad

Aviso:
Para ayudarle a utilizar mejor los productos y servicios de ZKTeco (en adelante, "nosotros", "nuestro" o "nos"), proveedor de servicios inteligentes, recopilamos su información personal de forma sistemática. Entendemos la importancia de su información personal, por lo que nos tomamos muy en serio su privacidad y hemos formulado esta política de privacidad para protegerla. A continuación, presentamos las políticas de privacidad para que comprenda con precisión las medidas de protección de datos y privacidad relacionadas con nuestros productos y servicios inteligentes.
Antes de utilizar nuestros productos y servicios, lea atentamente y comprenda todas las normas y disposiciones de esta Política de Privacidad.Si no está de acuerdo con el acuerdo pertinente o alguno de sus términos ,Debes dejar de utilizar nuestros productos y servicios.

I.Información recopilada

Para garantizar el funcionamiento normal del producto y ayudar a la mejora del servicio, recopilaremos la información proporcionada voluntariamente por usted o proporcionada según su autorización durante el registro y el uso o generada como resultado de su uso de los servicios.

1.Información de registro de usuario:En su primer registro, la plantilla de funciones (Plantilla de huella dactilar/Plantilla de cara/Plantilla de palma) se guardará en el dispositivo según el tipo de dispositivo seleccionado para verificar la similitud única entre usted y el ID de usuario registrado. Opcionalmente, puede ingresar su nombre y código. Esta información es necesaria para usar nuestros productos. Si no la proporciona, no podrá usar algunas funciones del producto con regularidad.

2.Información del producto:De acuerdo con el modelo del producto y el permiso que usted otorgó cuando instala y utiliza nuestros servicios, la información relacionada con el producto en el que se utilizan nuestros servicios se recopilará cuando el producto se conecte al software, incluido el modelo del producto, el número de versión del firmware, el número de serie del producto y la información de capacidad del producto.Cuando conecte su producto al software, lea atentamente la política de privacidad del software específico.

II.Seguridad y gestión de productos

1.Al utilizar nuestros productos por primera vez, deberá configurar los privilegios de Administrador antes de realizar operaciones específicas. De lo contrario, se le recordará con frecuencia que configure los privilegios de Administrador al acceder a la interfaz del menú principal.Si aún no configura el privilegio de Administrador después de recibir el aviso del sistema, debe tener en cuenta el posible riesgo de seguridad (por ejemplo, los datos pueden modificarse manualmente).

2.Todas las funciones para mostrar información biométrica están deshabilitadas en nuestros productos por defecto. Puede seleccionar Menú > Ajustes del sistema para configurar si desea mostrar la información biométrica. Si habilita estas funciones, asumimos que conoce los riesgos de seguridad para la privacidad personal especificados en la política de privacidad.

3.De forma predeterminada, solo se muestra su ID de usuario. Puede configurar si desea mostrar otra información de verificación de usuario (como nombre, departamento, foto, etc.) con privilegios de administrador. Si elige mostrar dicha información, asumimos que es consciente de los posibles riesgos de seguridad (por ejemplo, su foto se mostrará en la interfaz del dispositivo).

4.La función de cámara está desactivada en nuestros productos por defecto. Si desea activar esta función para tomarse fotos a sí mismo para registrar la asistencia o a desconocidos para el control de acceso, el producto activará el tono de aviso de la cámara.Una vez que habilite esta función, asumimos que es consciente de los posibles riesgos de seguridad.

5.Todos los datos recopilados por nuestros productos se cifran mediante el algoritmo AES 256. Todos los datos que el Administrador carga en nuestros productos se cifran automáticamente mediante el algoritmo AES 256 y se almacenan de forma segura. Si el Administrador descarga datos de nuestros productos, asumimos que usted necesita procesarlos y que conoce el posible riesgo de seguridad. En tal caso, usted será responsable de almacenarlos. Debe saber que algunos datos no se pueden descargar por motivos de seguridad.

6.Toda la información personal de nuestros productos se puede consultar, modificar o eliminar. Si ya no utiliza nuestros productos, borre sus datos personales.

III.Cómo manejamos la información personal de menores

Nuestros productos, sitio web y servicios están diseñados principalmente para adultos. Los menores no podrán crear su propia cuenta sin el consentimiento de sus padres o tutores. Si es menor de edad, le recomendamos que pida a sus padres o tutores que lean atentamente esta Política y que utilice nuestros servicios o la información que le proporcionamos únicamente con el consentimiento de sus padres o tutores.
Solo utilizaremos o divulgaremos información personal de menores recopilada con el consentimiento de sus padres o tutores si y en la medida en que dicho uso o divulgación esté permitido por la ley o hayamos obtenido el consentimiento explícito de sus padres o tutores, y dicho uso o divulgación sea con el propósito de proteger a los menores.

Al observar que hemos recopilado información personal de menores sin el consentimiento previo de padres verificables, eliminaremos dicha información lo antes posible.

IV.Otros

Puedes visitarnoshttps://www.zkteco.com/cn/index/Index/protección_de_privacidad.html Para obtener más información sobre cómo recopilamos, usamos y almacenamos de forma segura su información personal.
Para mantenernos al día con el rápido desarrollo tecnológico, la adaptación de las operaciones comerciales y satisfacer las necesidades de los clientes, revisaremos y optimizaremos constantemente nuestras medidas y políticas de protección de la privacidad. Le invitamos a visitar nuestro sitio web oficial en cualquier momento para consultar nuestra política de privacidad más reciente.

Operación ecológica

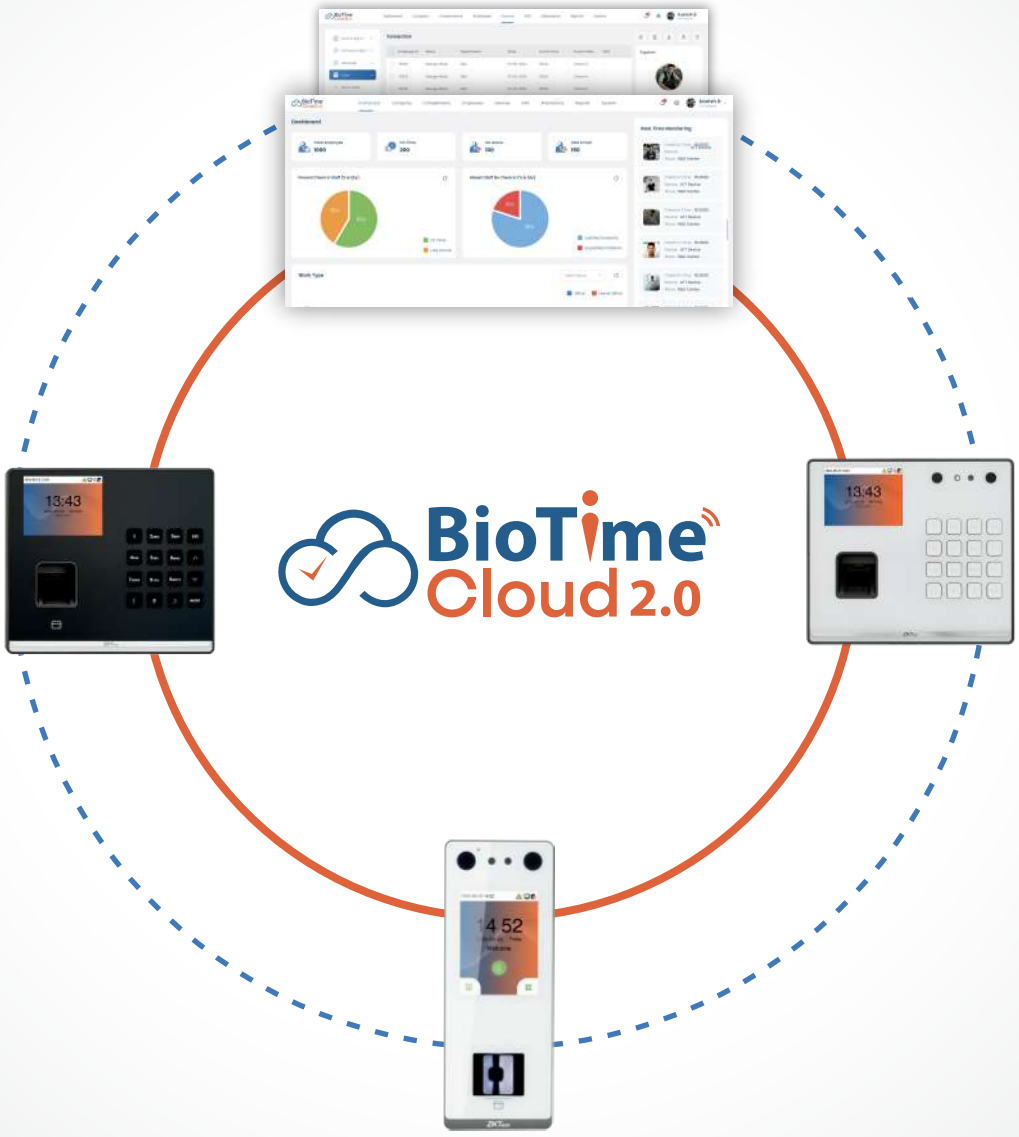
El "período operativo ecológico" del producto se refiere al tiempo durante el cual este producto no descargará ninguna sustancia tóxica o peligrosa cuando se utiliza de acuerdo con los requisitos previos de este manual.
El periodo de funcionamiento ecológico especificado para este producto no incluye baterías ni otros componentes que se desgastan fácilmente y deben reemplazarse periódicamente. El periodo de funcionamiento ecológico de la batería es de 5 años.

Sustancias peligrosas o tóxicas y sus cantidades

Componente Nombre	Sustancia/elemento peligroso/tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmio eh (Cd)	Hexava-lente cromo (Cr6+)	Polibromado d Bifenilos (PBB)	Polibromados Éteres de difenilo (PBDE)
Resistencia de chip	×	○	○	○	○	○
Condensador de chip	×	○	○	○	○	○
Inductor de chip	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
ESD componente	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Tornillos	○	○	○	×	○	○

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

ZKTeco



Your AI Workforce Cloud Attendance Management Platform

www.zkteco.com

www.zkteco.mx

Copyright © 2024 ZKTECO CO., LTD. All rights reserved.