MANUAL DE USUARIO

Modelos aplicables: G4L

Versión: 1.1

Fecha: julio de 2020

Inglés

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

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

Marca comercial

ZKTeco es una marca registrada de ZKTECO CO., LTD. Otras marcas comerciales involucradas en este manual son propiedad de sus respectivos dueños.

Descargo de responsabilidad

Este manual contiene información sobre el funcionamiento y mantenimiento del producto ZKTeco. Los derechos de autor de todos los documentos, dibujos, etc. en relación con el producto suministrado por ZKTeco pertenecen y son propiedad de ZKTeco. El receptor no debe usar ni compartir el contenido del presente con ningún tercero sin el permiso expreso por escrito de ZKTeco.

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

Es un prerrequisito esencial para la operación y el mantenimiento satisfactorios que el personal de operación y mantenimiento esté completamente familiarizado con el diseño y que dicho personal haya recibido una formación completa en la operación y mantenimiento de la máquina / unidad / producto. Además, es esencial para el funcionamiento seguro de la máquina / unidad / producto que el personal haya leído, entendido y seguido las instrucciones de seguridad contenidas en el manual.

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

ZKTeco no ofrece garantía, garantía o representación con respecto a la integridad de cualquier información contenida en este manual o cualquiera de las enmiendas realizadas al 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 por ningún error u omisión en la información o los documentos a los que se hace referencia o están vinculados a este manual. El usuario asume todo el riesgo en cuanto a los resultados y el rendimiento obtenido del uso de la información.

ZKTeco en ningún caso será responsable ante el usuario o cualquier tercero por cualquier daño incidental, consecuente, indirecto, especial o ejemplar, incluyendo, sin limitación, pérdida de negocio, lucro cesante, interrupción del negocio, pérdida de información comercial o cualquier pérdida pecuniaria, que surja de, en conexión con, o relacionada con el uso de la información contenida o referenciada en este manual, incluso si ZKTeco ha sido advertido de la posibilidad de tales daños.

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

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

El producto se actualizará de vez en cuando sin previo aviso. Los últimos procedimientos operativos y documentos relevantes están disponibles en http: // www. zkteco .com

Si hay algún problema relacionado con el producto, comuníquese con nosotros.

Sede de ZKTeco

Habla a Parque Industrial ZKTeco, No. 26, 188 Industrial Road,

Ciudad de Tangxia, Dongguan, China.

Teléfono +86769 - 82109991

Fax + 86 755 - 89602394

Para consultas relacionadas con el negocio, escríbanos a: sales@zkteco.com . Para saber más

sobre nuestras sucursales globales, visite www.zkteco.com .

Sobre la empresa

ZKTeco es uno de los fabricantes más grandes del mundo de lectores RFID y biométricos (huellas dactilares, faciales, venas dactilares). Las ofertas de productos incluyen lectores y paneles de control de acceso, cámaras de reconocimiento facial de rango cercano y lejano, controladores de acceso a elevadores / pisos, torniquetes, controladores de puertas de reconocimiento de matrículas (LPR) y productos de consumo que incluyen cerraduras de puertas con lector de huellas dactilares y faciales a batería. Nuestras soluciones de seguridad son multilingües y están localizadas en más de 18 idiomas diferentes. En el estado de la técnica de ZKTeco

Planta de fabricación de 700,000 pies cuadrados con certificación ISO9001, controlamos la fabricación, el diseño de productos, el ensamblaje de componentes y la logística / envío, todo bajo un mismo techo.

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

Acerca del manual

Este manual presenta las operaciones de **G4L** producto.

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

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

Convenciones de documentos

Las convenciones utilizadas en este manual se enumeran a continuación:

Convenciones GUI

Para software	
Convención	**Descripción**
Negrita	Se utiliza para identificar nombres de interfaz de software, p. Ej. **Aceptar, confirmar, cancelar**
>	Los menús de varios niveles están separados por estos corchetes. Por ejemplo, Archivo> Crear> Carpeta.
Para dispositivo	
Convención	**Descripción**
<>	Nombres de botones o teclas para dispositivos. Por ejemplo, presione <OK>
[]	Los nombres de las ventanas, los elementos del menú, la tabla de datos y los nombres de los campos están entre corchetes. Por ejemplo, abre la ventana [Usuario nuevo]
/	Los menús de varios niveles están separados por barras diagonales. Por ejemplo, [Archivo / Crear / Carpeta].

Simbolos

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

Tabla de contenido

1 Medidas de seguridad

Las siguientes precauciones son para mantener la seguridad del usuario y evitar cualquier daño. Lea atentamente antes de la instalación.

1. **Lea, siga y conserve las instrucciones:** Todas las instrucciones de seguridad y funcionamiento deben estar correctamente leer y seguir antes de poner en servicio el dispositivo.
2. **No ignore las advertencias:** Siga todas las advertencias de la unidad y las instrucciones de funcionamiento.
3. **Accesorios -** Utilice solo accesorios recomendados por el fabricante o vendidos por el producto. No se deben utilizar accesorios no recomendados por el fabricante.
4. **Precauciones para la instalación** - No coloque este dispositivo sobre un soporte o marco inestable. Puede 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 se ve afectado el control del cable o de la conexión.
   - Cuando se derramó el líquido o se cayó un artículo en el sistema.
   - Si se expone al agua y / o inclemencias del tiempo (lluvia, nieve y más). Si el sistema no funciona
   - normalmente según las instrucciones de funcionamiento.

Simplemente cambie los controles definidos en las instrucciones de funcionamiento. El ajuste inadecuado de otros controles puede resultar en daños e involucrar a un técnico calificado para regresar el dispositivo a la operación normal.

7. **Piezas de repuesto -** Cuando se necesitan piezas de repuesto, los técnicos de servicio solo deben utilizar repuestos proporcionados por el proveedor. Los sustitutos no autorizados pueden provocar quemaduras, descargas eléctricas u otros peligros.
8. **Verificación de seguridad -** Al finalizar el trabajo de servicio o reparación en la unidad, solicite al técnico de servicio que realice verificaciones de seguridad para garantizar el funcionamiento correcto de la unidad.
9. **Fuentes de energía -** Utilice el sistema solo desde la fuente de alimentación de la etiqueta. Si no está claro el tipo de fuente de alimentación a utilizar, llame a su distribuidor.
10. **Rayo -** Se pueden instalar pararrayos externos para proteger contra tormentas eléctricas. Evita que los power-ups destruyan el sistema.

Los dispositivos deben instalarse en áreas con acceso limitado.

2 Visión general

Nuestro dispositivo G4L facilita a los usuarios acceder a las funciones de la nube, que incluyen la recopilación, el almacenamiento y el análisis de datos. Esto beneficia a la organización al almacenar la información de la plantilla Bio en el servidor en la nube, y los datos se pueden recuperar cuando sea necesario. Este producto nuestro proporciona soluciones de extremo a extremo, y la tecnología de la nube se beneficia de mantener actualizaciones y monitorear los datos en la nube en tiempo real.

Este producto se puede utilizar tanto para el control de acceso como para el sistema de asistencia, que está basado en la nube. Nuestro objetivo es hacer una plataforma única, con servicios de hardware y software a muy bajo costo, y al mismo tiempo, apoyar el desarrollo brindando acceso a través de diferentes plataformas como móvil y web.

Alcance

- Sincronización con Bio Cloud Software Easy
- Access
- Fácil integración
- Cifrado y protección de datos de varios niveles Implementación y
- configuración rápidas

3 Instrucciones de uso

Antes de entrar en las características del dispositivo y sus funciones, se recomienda estar familiarizado con los fundamentos siguientes.

3.1 Colocación de dedos

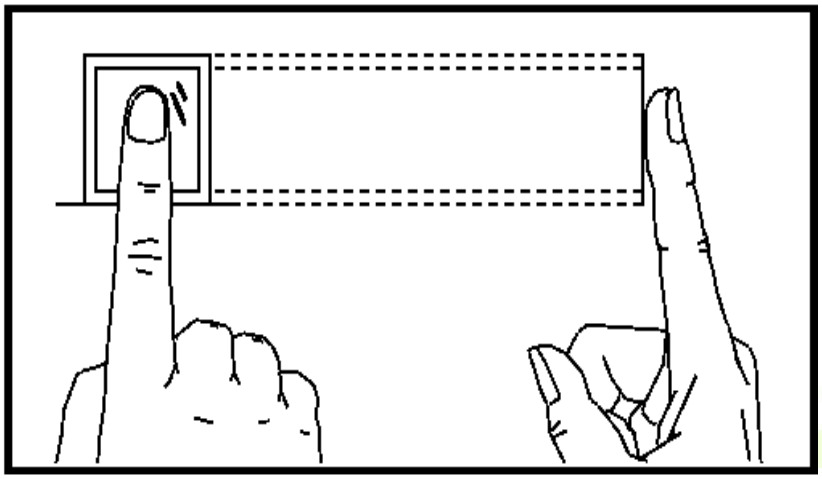
- Los dedos recomendados son los dedos índice, medio o anular.
- Evite usar el pulgar o el meñique, ya que son difíciles de presionar con precisión sobre el lector de huellas digitales.

Colocación correcta e incorrecta de los dedos

Recomendado

- Coloque el dedo en el área de escaneo y presiónelo sobre el lector de huellas digitales.
- Asegúrese de que el centro de su dedo esté alineado con el centro del lector de huellas digitales.

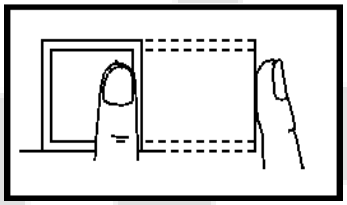
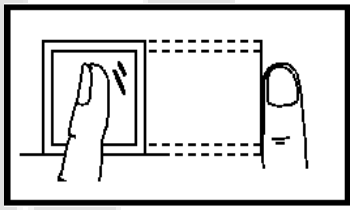
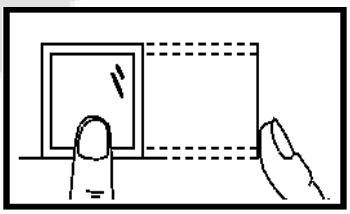
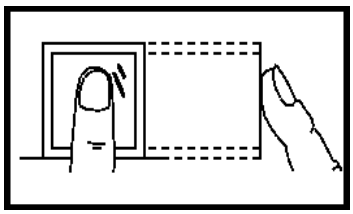
Representación esquemática



Colocación adecuada de los dedos en el lector de huellas dactilares

No recomendado

- Formas incorrectas de presionar el dedo sobre el lector de huellas dactilares.

Colocación de dedos	Descripción
	No se recomienda colocar el dedo lejos del centro del área de escaneo.
	No se recomienda colocar el dedo en los lados.
	No se recomienda colocar el dedo en una esquina del Área de escaneo.
	No se recomienda colocar el dedo en una posición elevada.

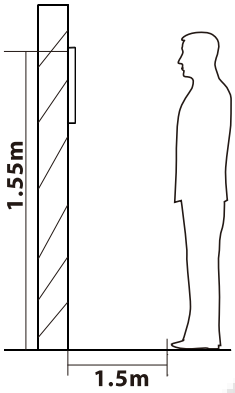
Nota:

- Se recomienda utilizar la ubicación adecuada de los dedos durante el proceso de inscripción y verificación.

- Nuestra empresa no asumirá ninguna responsabilidad por problemas de reconocimiento que puedan resultar del uso incorrecto del producto. Nos reservamos el derecho de interpretación final y modificación de este punto.

3.2 Posición de pie, expresión facial y postura de pie

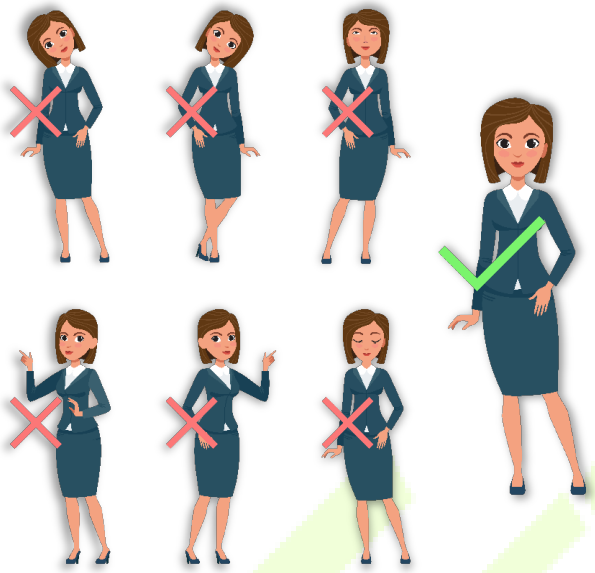
Distancia recomendada



La distancia entre el dispositivo y el usuario (cuya altura está dentro de 1,55 ma 1,85 m) se recomienda que sea de 1,5 m. Los usuarios pueden moverse ligeramente hacia adelante y hacia atrás para mejorar la calidad de las imágenes faciales capturadas.

Expresión facial recomendada

Posturas recomendadas de pie



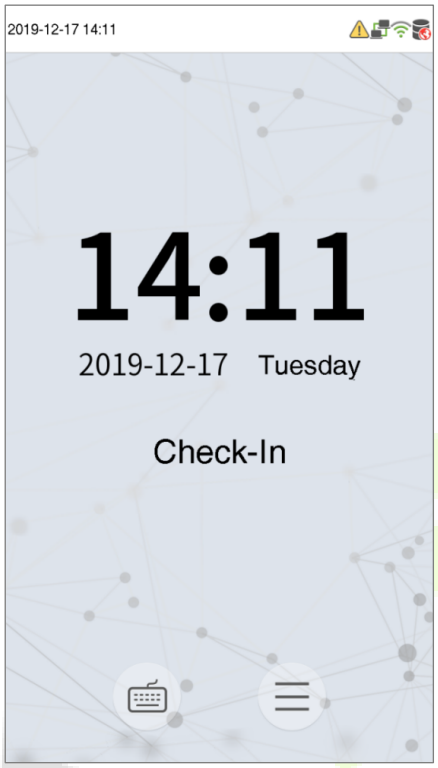
Nota: Durante el registro y la verificación, se recomienda mantener una expresión facial natural y una postura de pie.

3.3 Registro facial

Durante el registro, se recomienda mirar hacia la cámara y permanecer quieto en el centro de la pantalla del dispositivo como se muestra a continuación.

3.4 Interfaz de espera

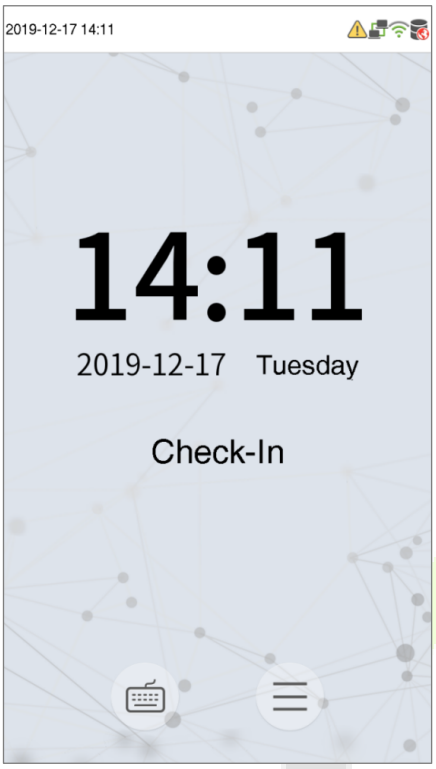
Después de conectar la fuente de alimentación, el dispositivo muestra la siguiente interfaz de espera.

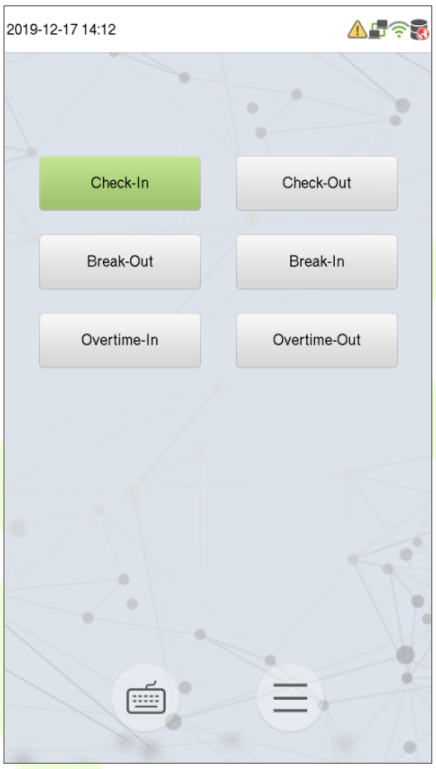


Notas:

- Toque en para ir a la interfaz de entrada de ID de usuario.
- Si el acceso de superadministrador no está configurado en el dispositivo, toque en para ir al menú.
- Si el superadministrador está configurado en el dispositivo, entonces se requiere la verificación del superadministrador para ir a las funciones del menú.
- Para la seguridad del dispositivo, se recomienda registrar el acceso de superadministrador por primera vez que utilice el dispositivo.

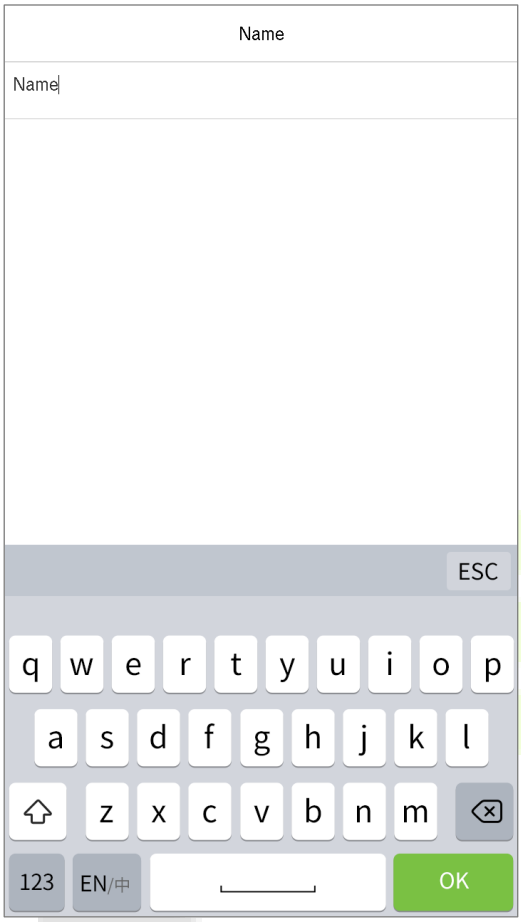
- El estado de marcado del dispositivo se puede configurar directamente mediante las teclas de acceso directo de la pantalla.





- Toque en cualquier lugar de la pantalla (sin tocar los iconos), para ver las seis opciones de estado de perforación como se muestra en la imagen de la derecha.
- Presione la tecla de método abreviado correspondiente para seleccionar el estado de perforación actual, que se muestra en verde. Por favor refiérase a " 7.5 Asignaciones de teclas de acceso directo "a continuación para el método de operación específico.

3,5 Teclado virtual



Nota:

Este dispositivo es compatible con chino, inglés, números y símbolos.

- Grifo [**ES]** para cambiar al teclado en inglés; Grifo [**123]** para cambiar al teclado
- de números y símbolos; Grifo [**A B C]** para volver al teclado alfabético. Toque el
- cuadro de entrada para el teclado virtual. Grifo [**ESC]** para salir de la entrada.
-
-

3.6 VerificationMode

El proceso de comparación biométrica se puede clasificar como, uno a muchos o "Identificación" (1: N), y uno a uno o "Verificación" (1: 1). A continuación se muestra una descripción de cada tipo de coincidencia y cómo se describen sus características.

Proceso de identificación 1: N

Un proceso de identificación biométrica de uno a muchos (1: N) compara instantáneamente la plantilla biométrica capturada de la persona con TODAS las plantillas biométricas almacenadas en el sistema.

Proceso de verificación 1: 1

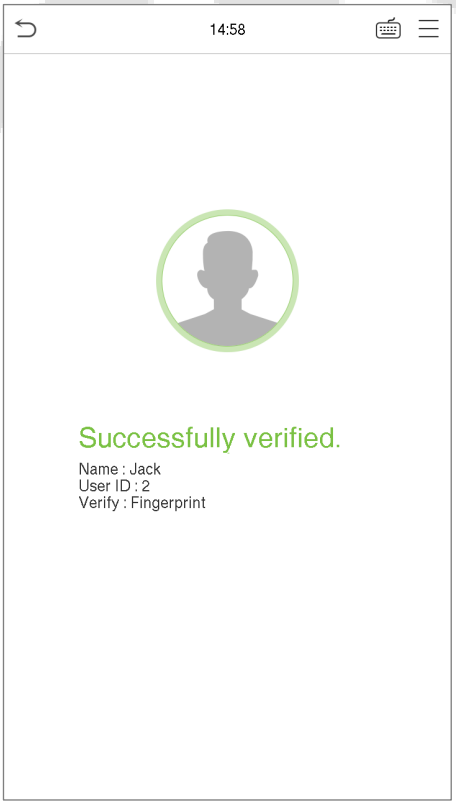
El proceso de verificación biométrica 1: 1 autentica la identidad de una persona al comparar la plantilla biométrica capturada con una plantilla biométrica de esa persona almacenada previamente en la base de datos.

3.6.1 Verificación de huellas dactilares

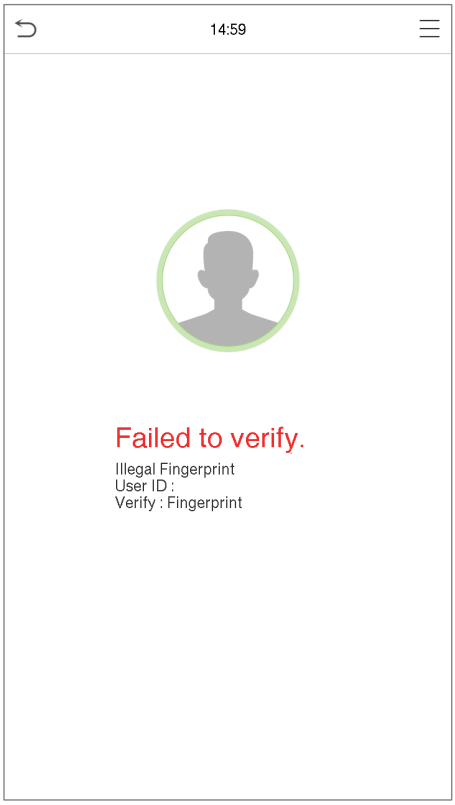
1: N proceso de identificación de huellas dactilares

- Este método compara la huella dactilar que se presiona y se escanea en el lector de huellas dactilares con todos los datos de huellas dactilares que se almacenan en el dispositivo.
- Una vez que el usuario presiona su dedo sobre el escáner de huellas dactilares, el dispositivo pasará al modo de autenticación de huellas dactilares. Es fundamental seguir la forma correcta de colocar el dedo en el sensor de huellas dactilares.

Verificación exitosa

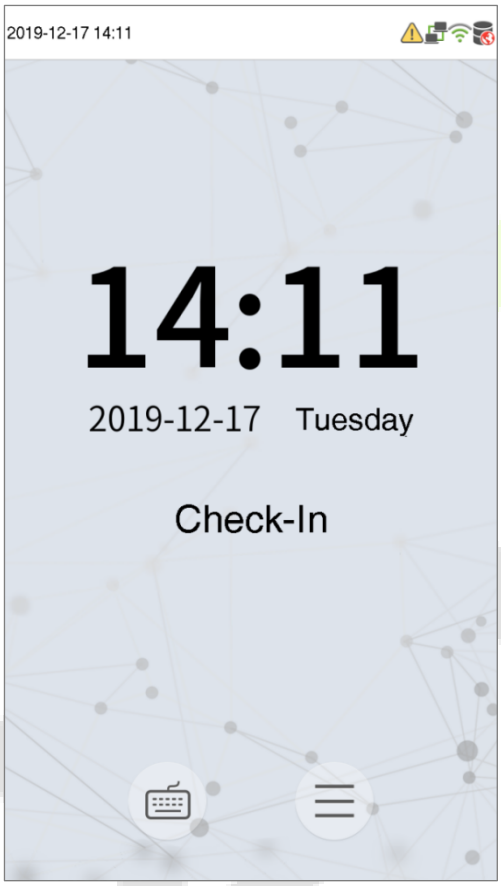


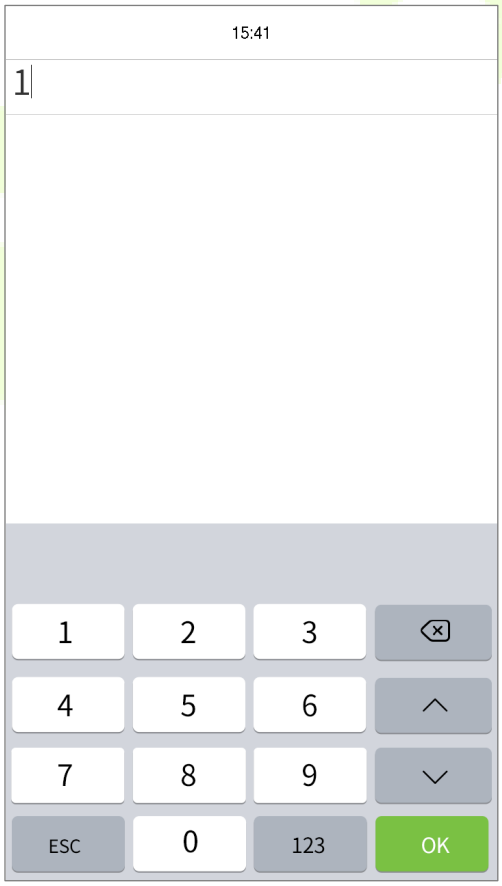
Verificación fallida



Proceso de verificación de huellas dactilares 1: 1

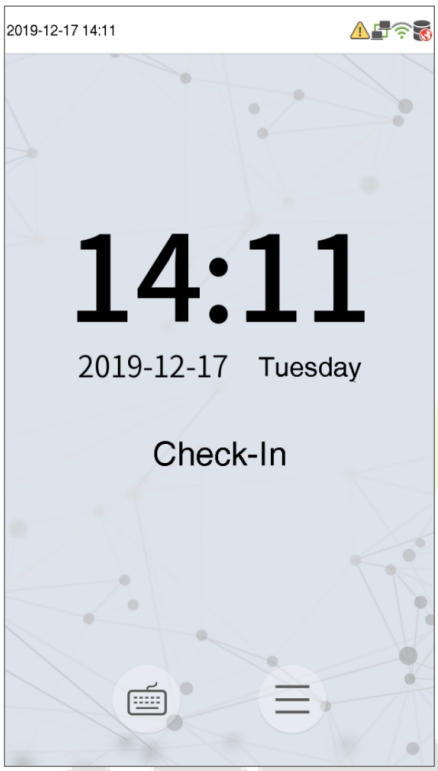
- Este método compara la huella dactilar que se presiona en el lector de huellas dactilares con las huellas dactilares que están vinculadas a la entrada de ID de usuario específica a través del teclado virtual.
- Los usuarios pueden intentar verificar sus identidades con el modo de verificación 1: 1 cuando no pueden acceder con el proceso de autenticación 1: N.
- En la pantalla principal, toque  para ir al modo de verificación de huellas dactilares 1: 1.
- En la pantalla, ingrese el ID de usuario y toque **OKAY.**

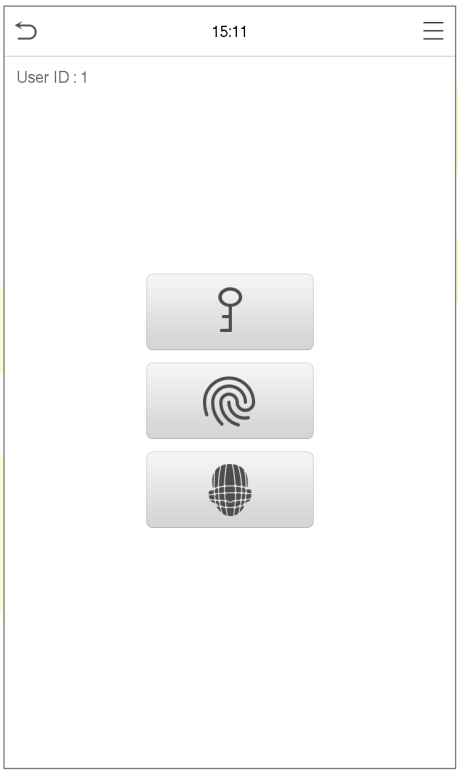




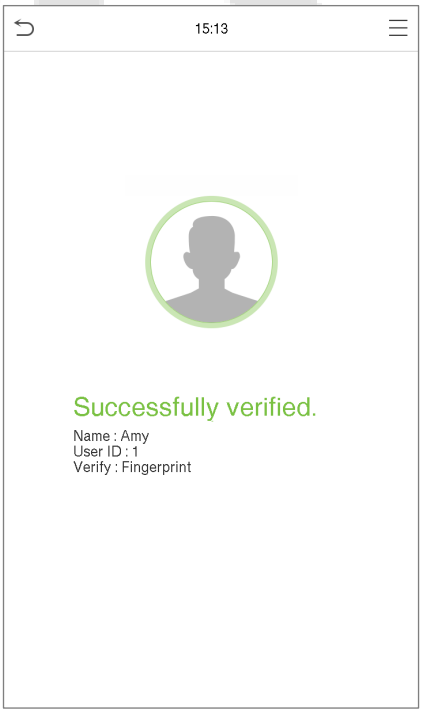
- Si el usuario ha registrado un rostro y una contraseña además de la huella digital, entonces el método de verificación se establece en huella digital / contraseña / verificación de rostro y aparecerá la siguiente pantalla en el Dispositivo.

- Toque en  icono de huella digital para ir al modo de verificación de huellas digitales y presione la huella digital para verificar.

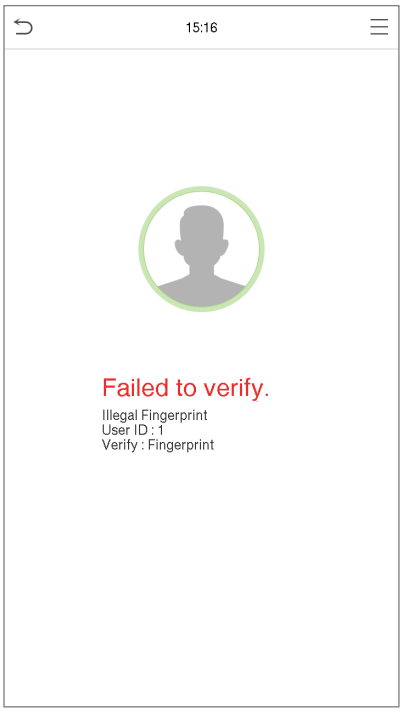




Verificación exitosa

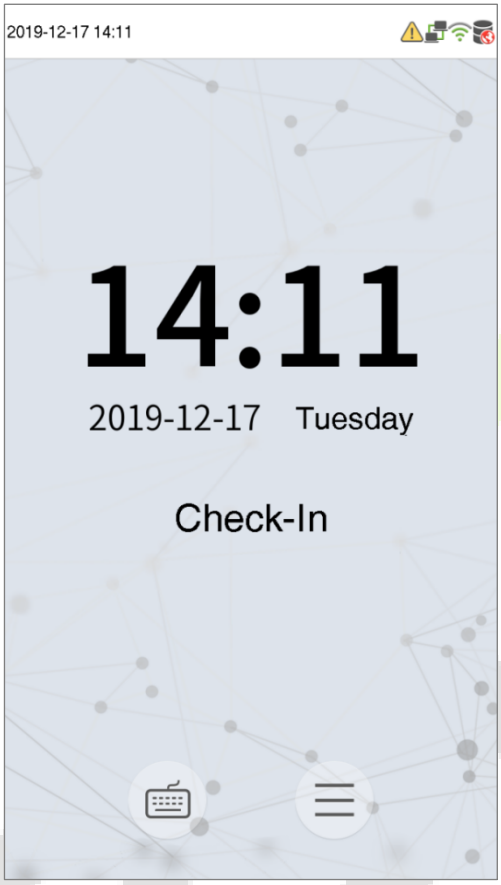


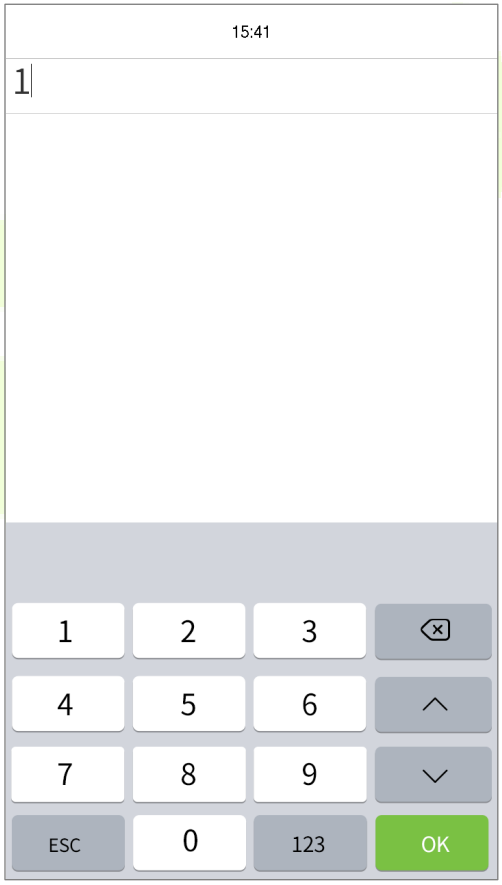
Verificación fallida



3.6.2 Verificación de contraseña

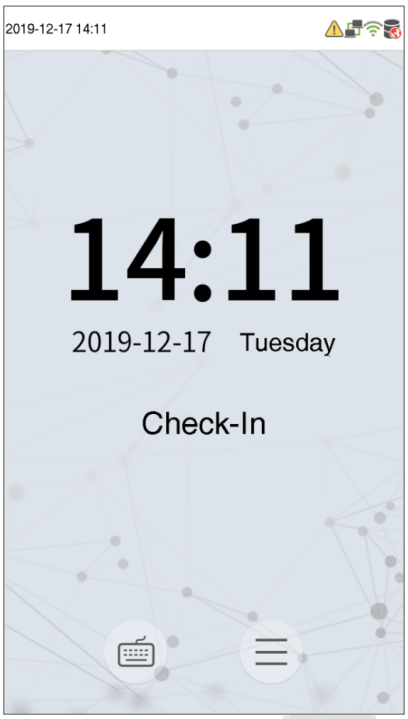
- Este método compara la contraseña ingresada con el ID de usuario y la contraseña registrados.
- En la pantalla de Menú, toque  para ir al modo de verificación de contraseña 1: 1.
- En la pantalla de entrada, ingrese la ID de usuario y presione **OKAY.**

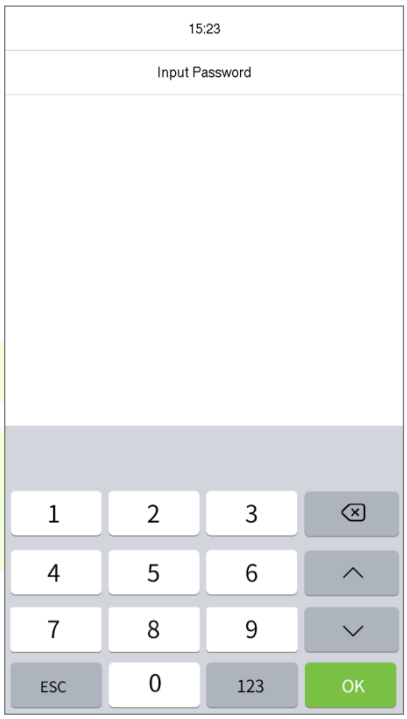




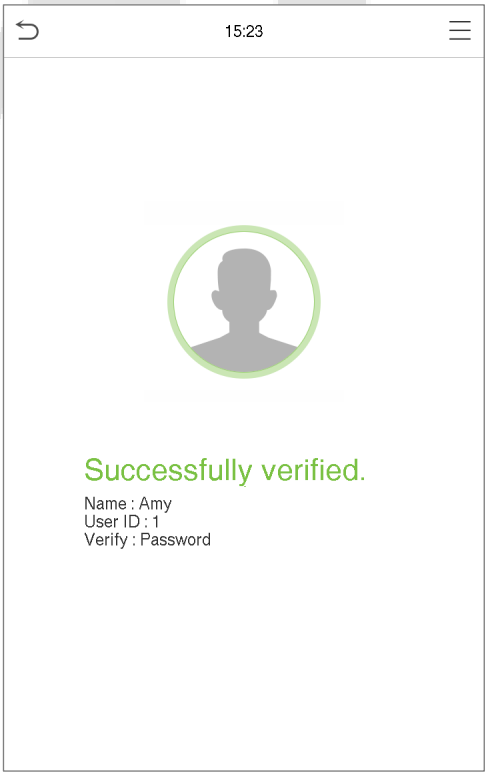
- Si el usuario ha registrado rostro y huella digital además de la contraseña, entonces el método de verificación se establece en huella digital / contraseña / verificación de rostro y aparecerá la siguiente pantalla en el Dispositivo.

- Toque en  el botón para ir al modo de verificación de contraseña, luego ingrese la contraseña, y luego toque **OKAY.**

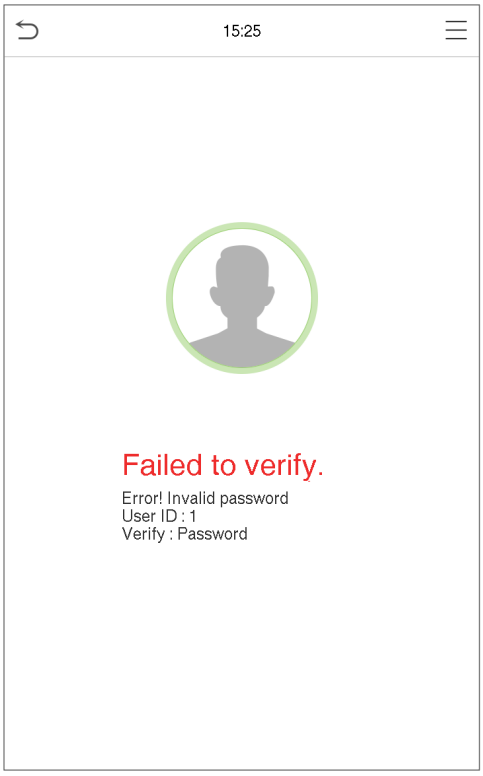




Verificación exitosa



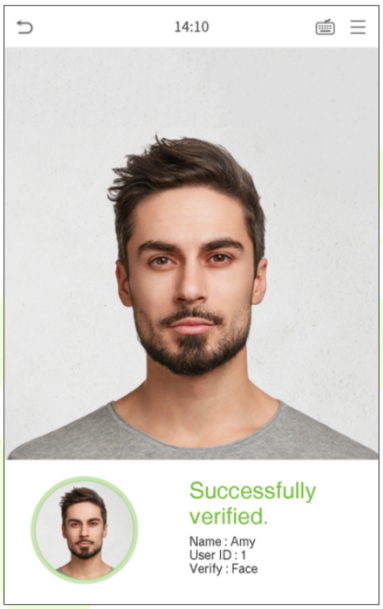
Verificación fallida



3.6.3 Verificación facial

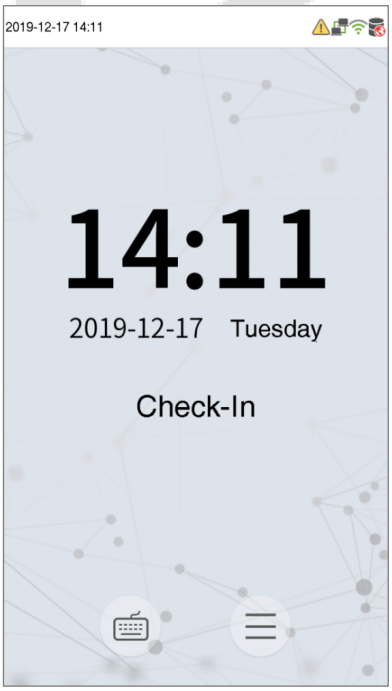
1: N identificación facial

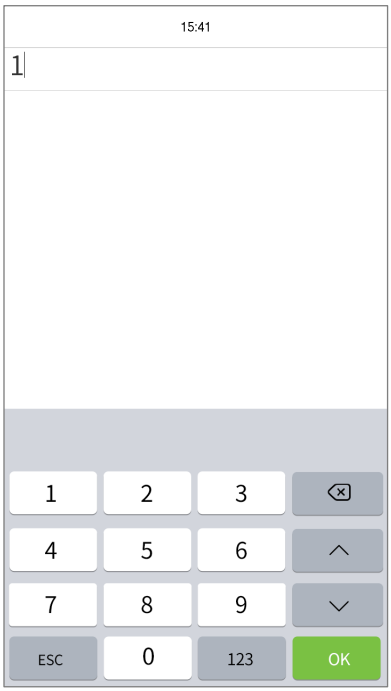
- Este método compara las imágenes faciales adquiridas con todos los datos faciales registrados en el dispositivo.
- El siguiente es el mensaje de solicitud del resultado de la comparación.



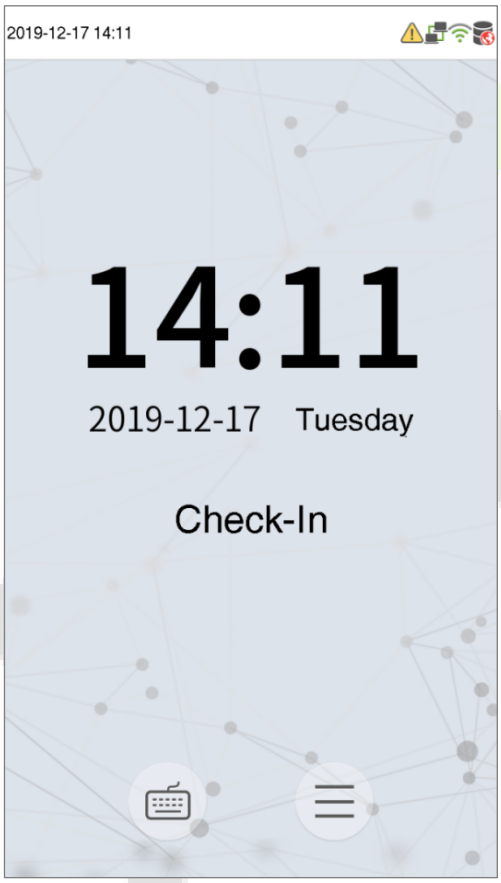
Verificación facial 1: 1

- Este método compara el rostro capturado por la cámara con la plantilla facial relacionada con el ID de usuario ingresado.
- En la interfaz principal, toque el botón para ir al modo de verificación facial 1: 1.





- Ingrese el ID de usuario y haga clic en **OKAY.**
- Si el usuario ha registrado una contraseña y una huella digital además de la cara, el método de verificación se establece en huella digital / contraseña / verificación facial y aparecerá la siguiente pantalla en el Dispositivo.
- Toque en el botón para ir al modo de verificación facial.
- Si el usuario ha registrado rostro y huella digital además de la contraseña, entonces el método de verificación se establece en huella digital / contraseña / verificación de rostro y aparecerá la siguiente pantalla en el Dispositivo.
- Toque en el botón para ir al modo de verificación de contraseña, luego ingrese la contraseña, y luego toque **OKAY.**



Después de una verificación exitosa, se mostrará el mensaje "verificado exitosamente".

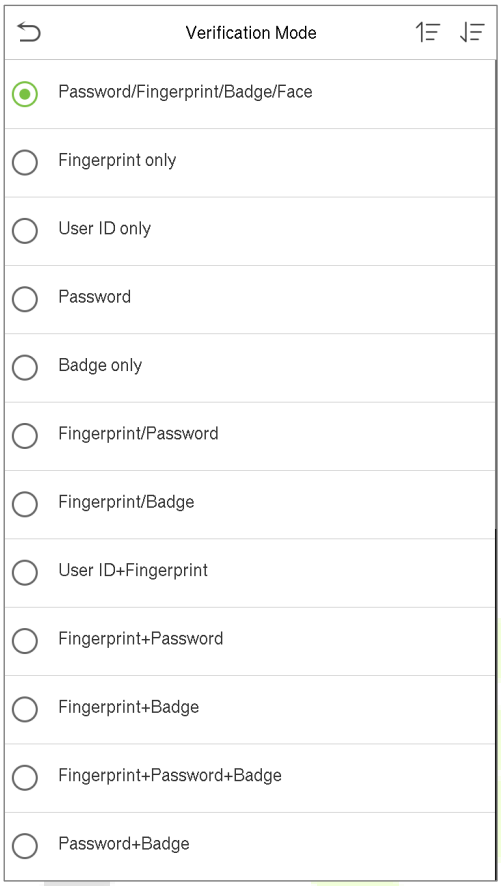
Si la verificación falla, aparecerá el mensaje "¡Por favor, ajuste su posición!" será mostrado.

3.6.4 Verificación combinada

Para aumentar la seguridad, este dispositivo ofrece la opción de utilizar múltiples formas de modo de verificación. En este dispositivo, se pueden utilizar un total de 11 combinaciones de verificación diferentes.

Definición de símbolo de verificación combinada

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

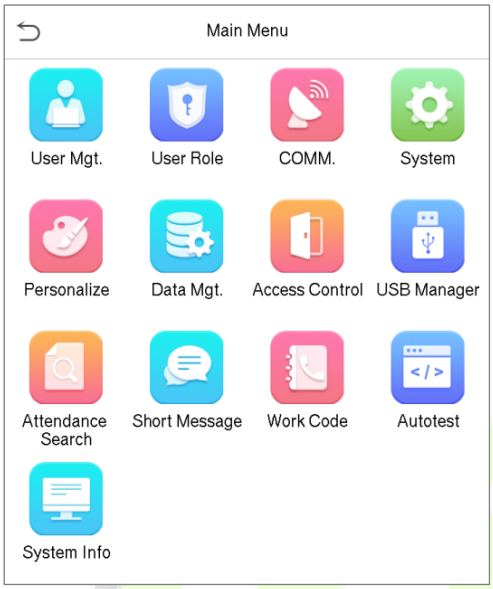


Procedimiento para configurar CombinedVerificationMode

- La verificación combinada requiere que el personal registre 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 de la huella digital, pero el modo de verificación del dispositivo está configurado como "Huella digital + contraseña", el empleado no podrá completar el proceso de verificación con éxito.
- Esto se debe a que el Dispositivo compara la plantilla de huella digital escaneada de la persona con la plantilla de verificación registrada (tanto la Huella digital como la Contraseña) almacenada previamente con esa ID de personal en el Dispositivo.
- Pero como el empleado ha registrado solo la huella digital, pero no la contraseña, la verificación no se completará y el dispositivo muestra "Verificación fallida".

4 Menú principal

- Sobre el **Colocarse** interfaz, toque en botón para ir al **Menú principal:**



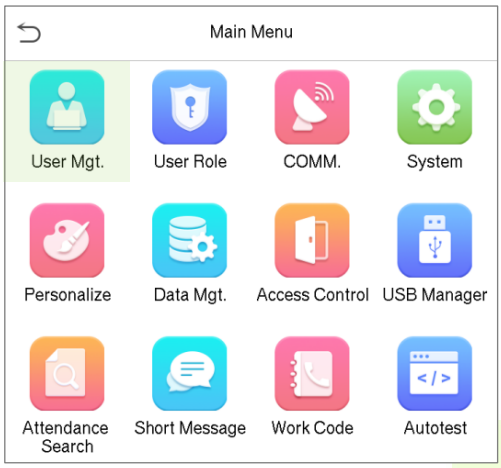
Operaciones de menú

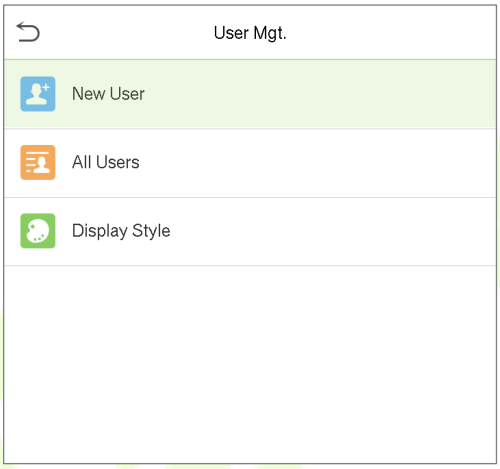
Menú	Descripciones
Administrador de usuarios	Para agregar, editar, ver y eliminar la información básica sobre un usuario.
Rol del usuario	Para establecer el alcance del permiso del rol personalizado, es decir, para establecer los derechos de acceso para operar el sistema.
COMM.	Para configurar los parámetros de red relevantes, la conexión de la PC, el servidor en la nube y los detalles de Wiegand.
Sistema	Para configurar los parámetros relacionados con el sistema, incluida la fecha y la hora, la configuración de los registros de asistencia / acceso, la cara, los parámetros de huellas dactilares, restablecer los valores de fábrica y la actualización USB.
Personalizar	Para personalizar la configuración de la pantalla de la interfaz, voz, timbre, opciones de estado de marcado y teclas de acceso directo.
DataMgt.	Para eliminar todos los datos relevantes en el dispositivo.
Control de acceso	Para configurar los parámetros de la cerradura y el dispositivo de control de acceso correspondiente.
USBManager	Touploador descargar datos específicos de un USBdrive.
Búsqueda de asistencia	Consulte el registro de asistencia específico, verifique las fotos de asistencia y las fotos de la lista negra. Agregar / verificar /
Mensaje corto	editar / eliminar mensajes públicos y personales. Establecer opciones.
Código de trabajo	Tomar diferentes categorías de trabajo, facilitando el control de asistencia del usuario.
Auto prueba	Para probar automáticamente si cada módulo funciona correctamente, incluida la pantalla LCD, la voz, el sensor de huellas dactilares, la cámara y el reloj RTC.
Información del sistema	Para ver la capacidad de datos, el dispositivo y la información de firmware del dispositivo actual.

5 Gestión de usuarios

5.1 registro de usuario

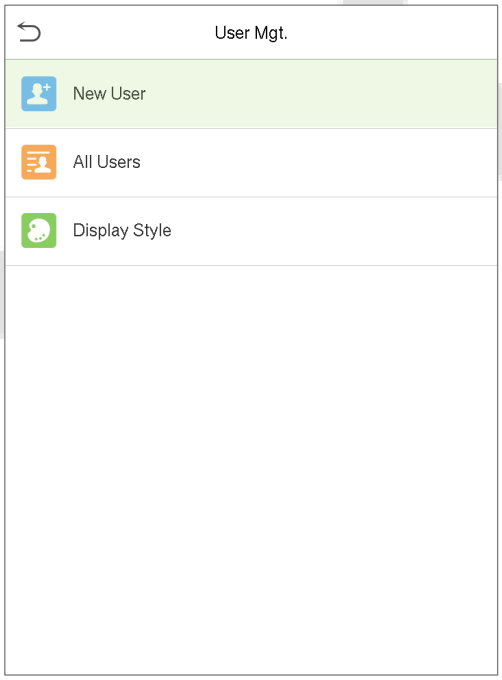
- Sobre el **Principal** menú, toque **Gestión de usuarios,** y luego toque **Nuevo Usuario** para agregar un nuevo usuario.

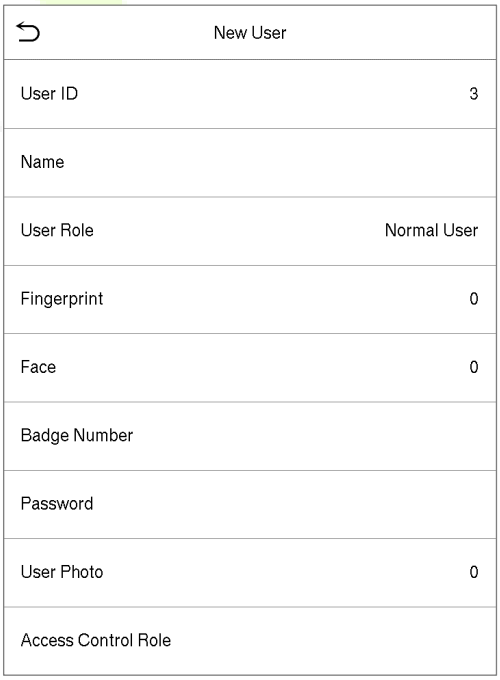




5.1.1 ID de usuario y nombre

- Sobre el **Nuevo Usuario** interfaz, ingrese **ID de usuario** y **Nombre.**



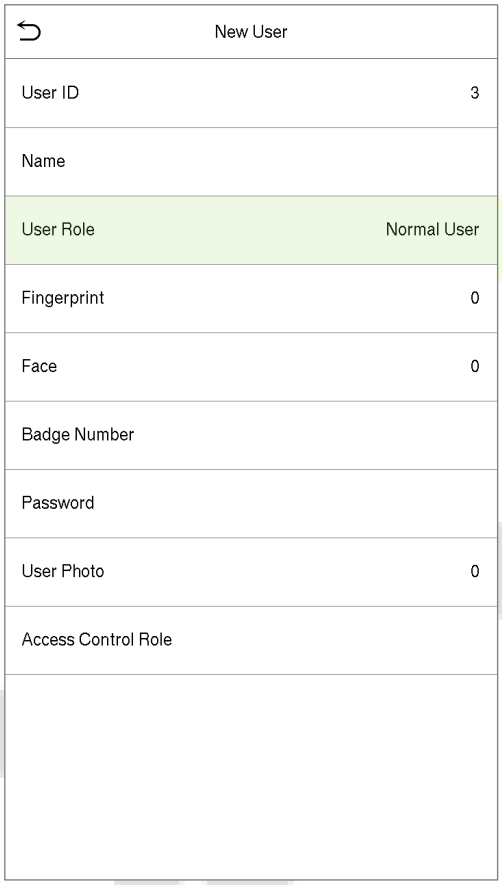


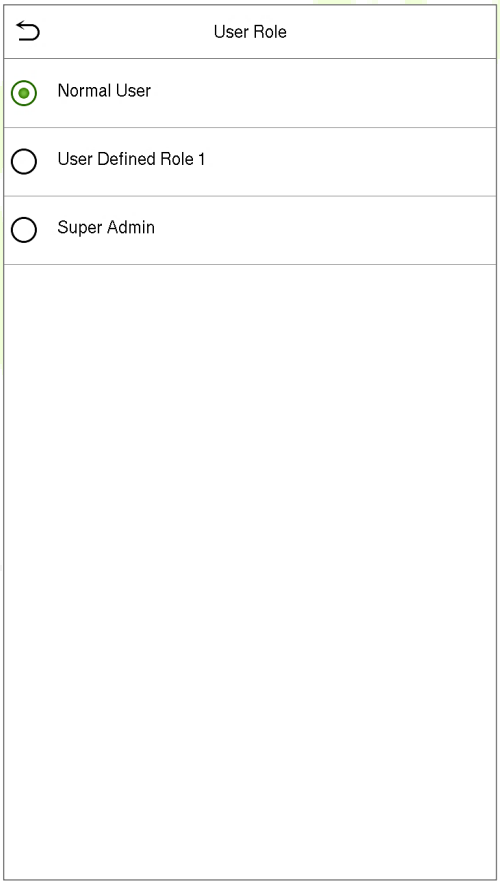
Notas:

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

5.1.2 Rol del usuario

- En la interfaz de nuevo usuario, toque **Rol del usuario** para establecer el rol del usuario como **Usuario normal** o **Super administrador.**
- **Superadministrador:** El superadministrador posee todos los privilegios de administración en el dispositivo.
- **Usuario normal:** Si el superadministrador ya está registrado en el dispositivo, 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:** El usuario normal también se puede configurar con **Rol definido por el usuario** que son los roles personalizados que se pueden configurar para el usuario normal.

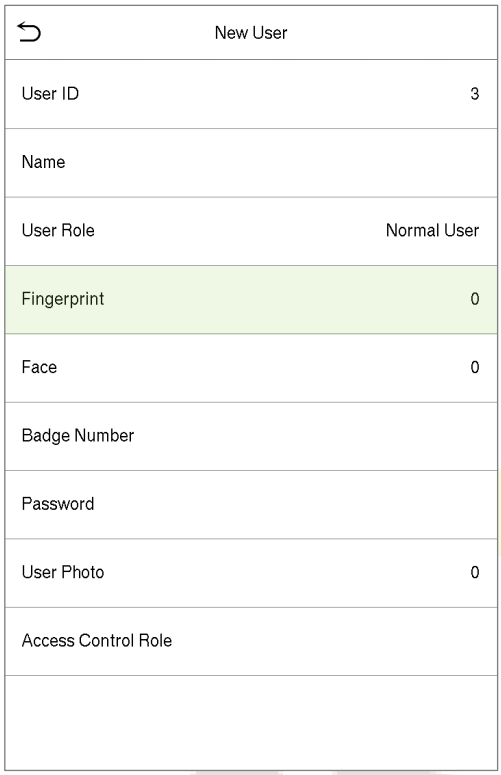


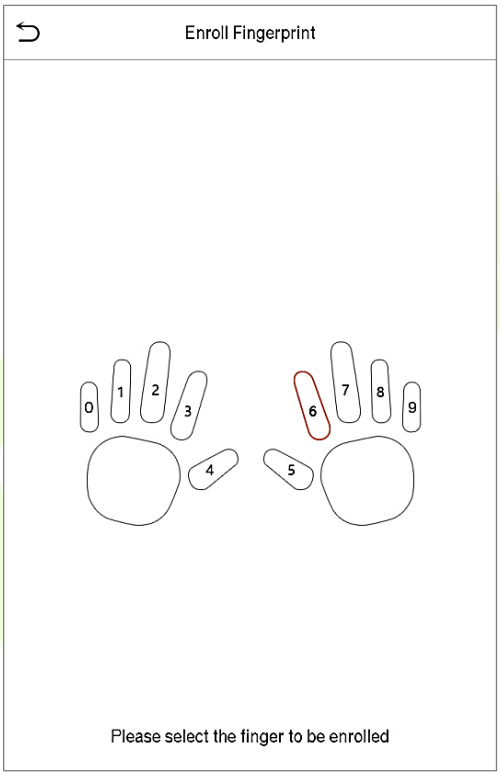


Nota: Si el rol de usuario seleccionado es el superadministrador, solo el superadministrador puede proporcionar la autenticación de identidad para acceder al menú principal. La autenticación se basa en la verificación método (s) que el superadministrador ha registrado.

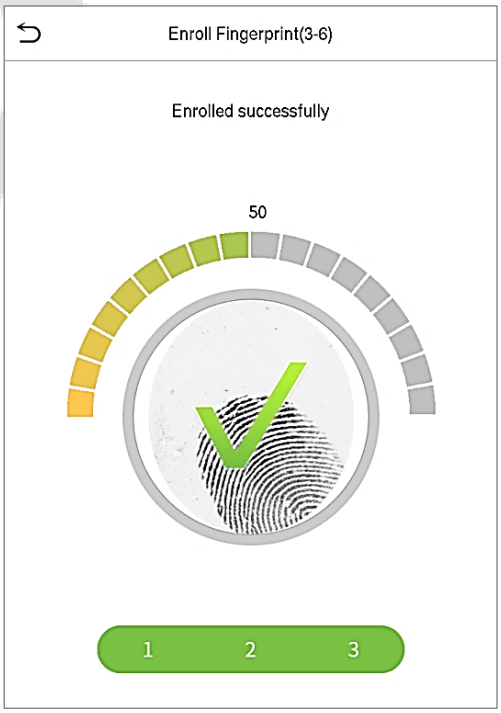
5.1.3 Huella dactilar

- Sobre el **Nuevo Usuario** interfaz, toque en **Huella dactilar** para ir a la página de registro de huellas digitales.
- Sobre el **Inscribir huella digital** interfaz, seleccione el dedo a registrar.



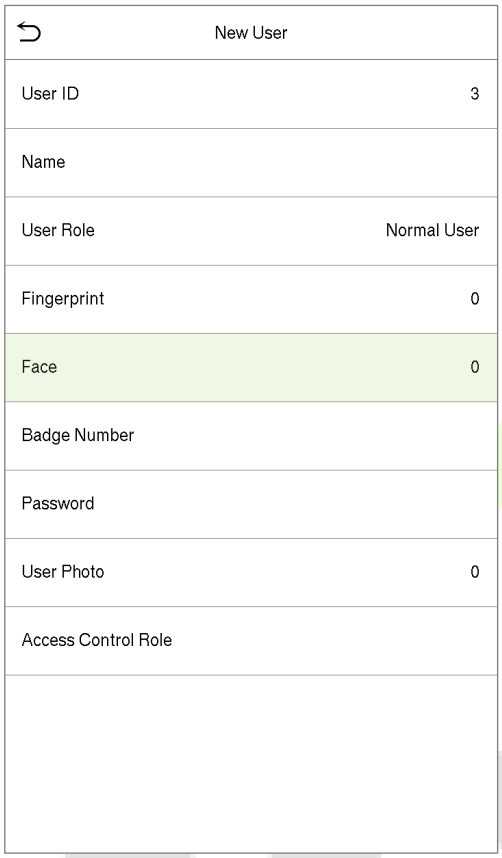


- Después de seleccionar el dedo requerido, presione el mismo dedo en el lector de huellas dactilares tres veces.
- El verde indica que la huella digital se registró correctamente.



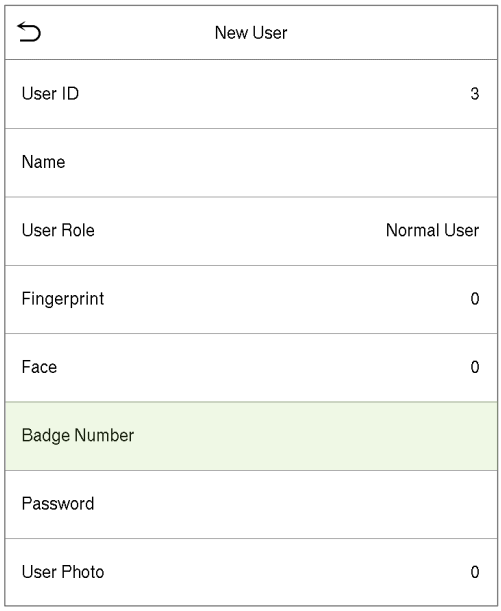
5.1.4 Cara

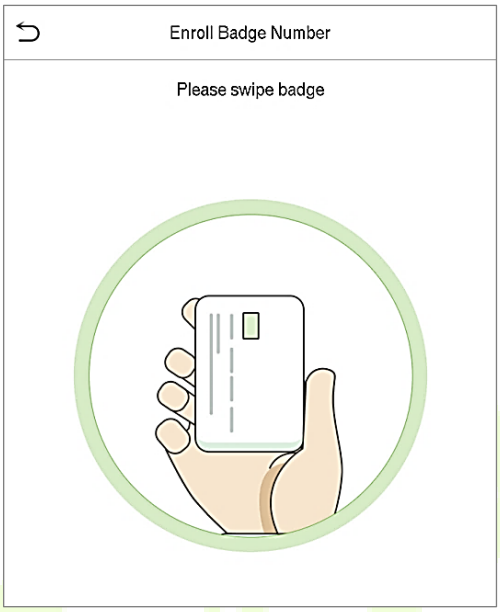
- Sobre el **Nuevo Usuario** interfaz, toque en **Cara** para ingresar a la página de registro facial.
- Durante el proceso de registro facial, el usuario debe mirar a la cámara y permanecer quieto como se muestra a continuación.



5.1.5 Numero de placa

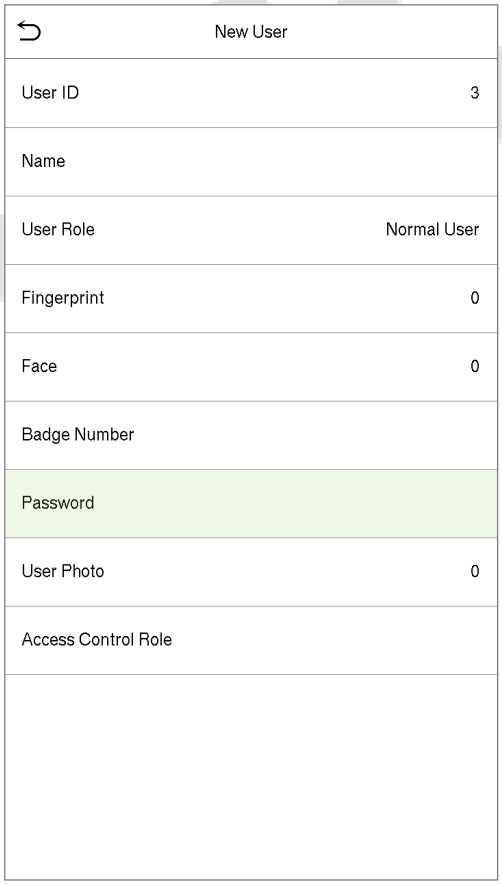
- Sobre el **Nuevo Usuario** interfaz, toque en **Numero de placa** para ir a la página de registro del número de placa.
- Sobre el **Inscribir número de placa** interfaz, el usuario debe deslizar la insignia en el lector de tarjetas IC para registrar el número de tarjeta.

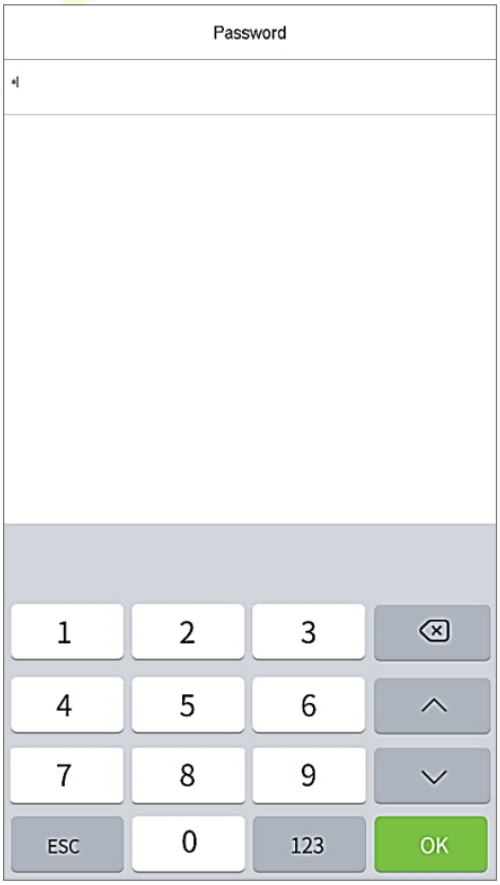




5.1.6 Contraseña

- Sobre el **Nuevo Usuario** interfaz, toque en **Contraseña** para ir a la página de registro de contraseña.
- En la interfaz de Contraseña, ingrese la contraseña requerida y vuelva a ingresar para confirmarla y toque **OKAY.**
- Si la contraseña reingresada es diferente de la contraseña ingresada inicialmente, entonces el dispositivo muestra el mensaje "Contraseña no coincide", donde el usuario debe volver a confirmar la contraseña nuevamente.

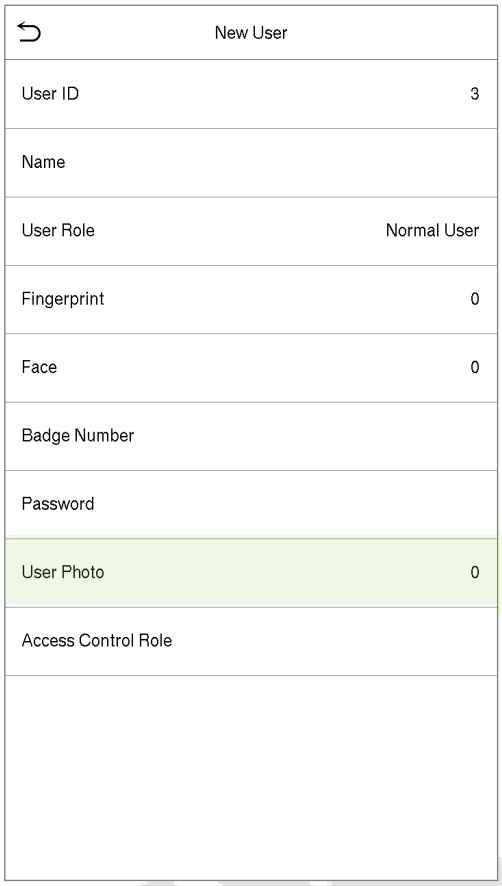




Nota: La contraseña puede contener de 1 a 8 dígitos por defecto.

5.1.7 Foto de usuario

- Sobre el **Nuevo Usuario** interfaz, toque en **Foto de usuario** para ir a la página de registro de fotos de usuario.



- Cuando un usuario registrado con una foto pasa la autenticación, se mostrará la foto registrada.

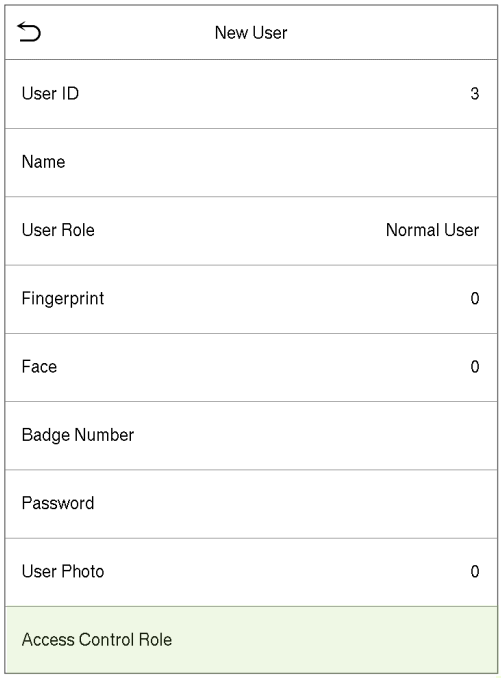
- Grifo **Foto de usuario,** toque el botón de la cámara para tomar una foto. El sistema volverá a la interfaz de nuevo usuario después de hacer clic en la foto.

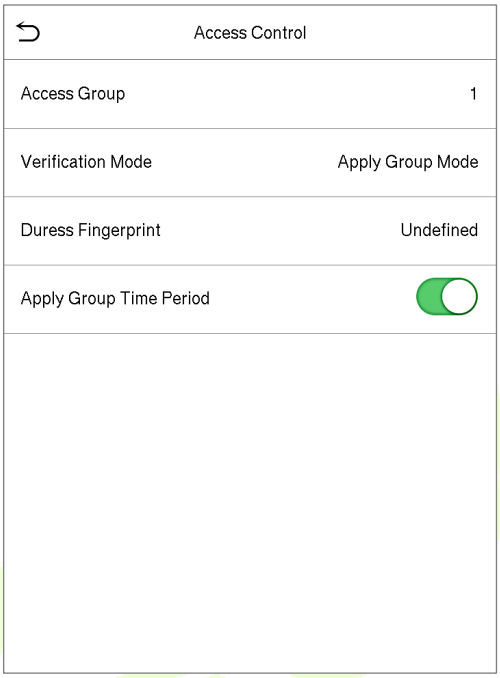
Nota: Al registrarse para la cara, el sistema capturará automáticamente la imagen del usuario y la establecerá como la foto del usuario de forma predeterminada. Por lo tanto, incluso si el usuario no desea registrar una foto de usuario, el sistema establecerá automáticamente la imagen capturada como la foto de usuario predeterminada.

5.1.8 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, el modo de verificación, el privilegio de huellas digitales y también facilita la configuración del período de tiempo de acceso del grupo.

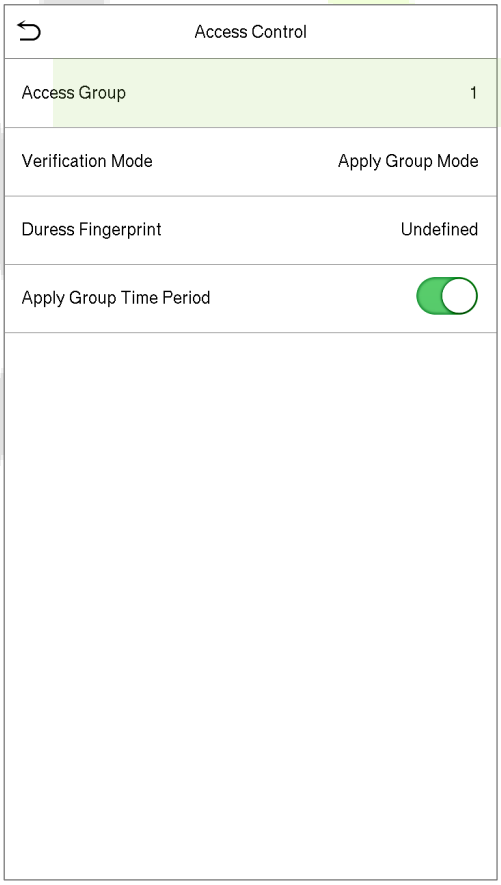
- Sobre el **Nuevo Usuario** interfaz, toque en **Rol de control de acceso** para ir a la interfaz de Control de acceso.





Establecer el grupo de acceso

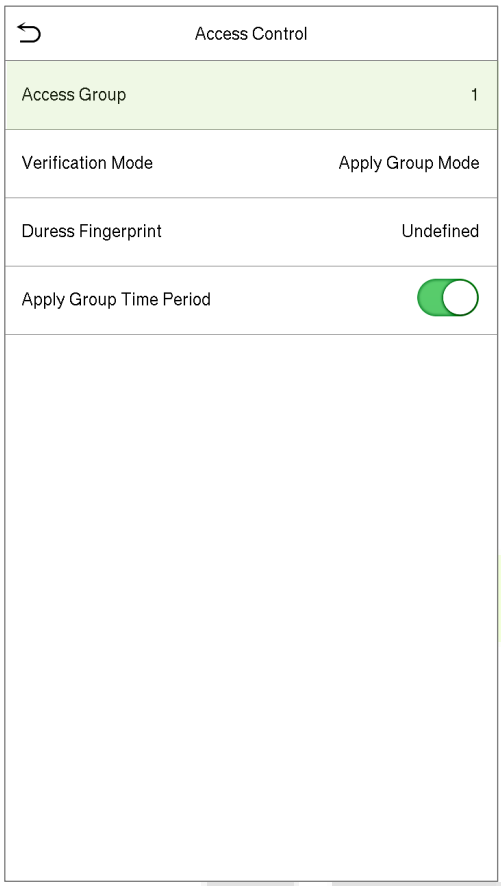
- Sobre el **Rol de control de acceso,** toque en **Grupo de acceso** asignar a los usuarios registrados a diferentes grupos para una mejor gestión.

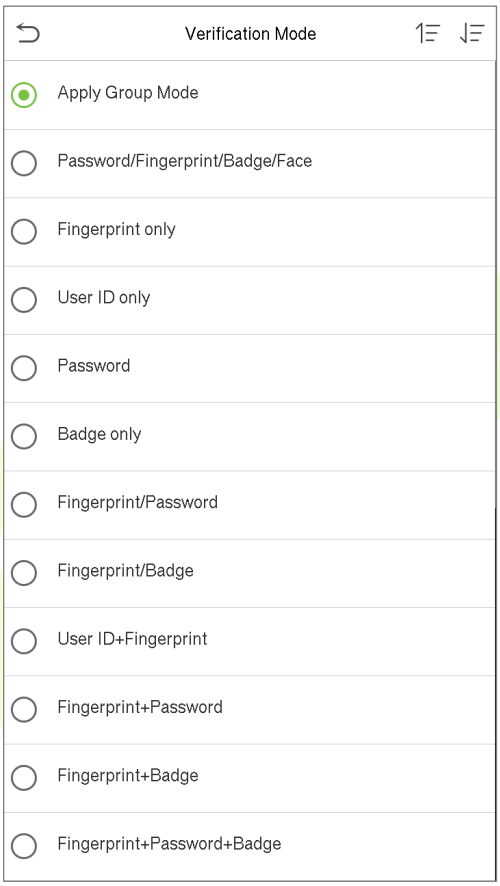


- Los nuevos usuarios se agregarán al Grupo 1 de forma predeterminada, que se puede reasignar a otros grupos necesarios.
- El dispositivo admite hasta 99 grupos de control de acceso.

Establecer el modo de verificación

- Sobre el **Grupo de acceso** interfaz, toque en **VerificationMode** para establecer el tipo de verificación para el usuario.

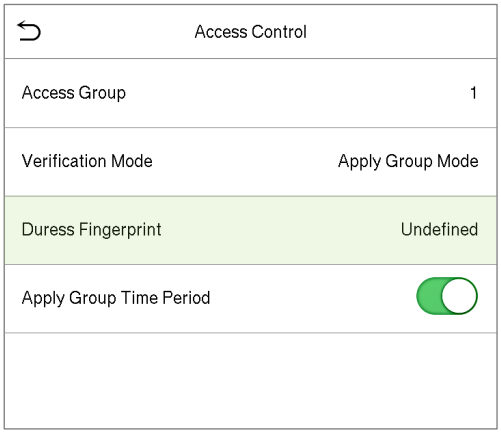




- Sobre el **VerificationMode** interfaz, seleccione el tipo de verificación requerido de la lista.

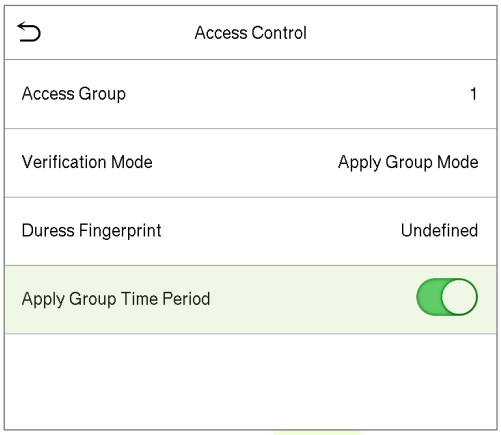
Huella dactilar de coacción

- En la Interfaz de control de acceso, toque Huella dactilar de coacción para ir a la página de huellas dactilares de coacción.
- El usuario puede especificar una o más huellas dactilares para registrarlas como huellas dactilares de coacción. Por lo tanto, una vez que el usuario presiona el dedo correspondiente en el sensor, y si la verificación es exitosa, el sistema generará inmediatamente la alarma.



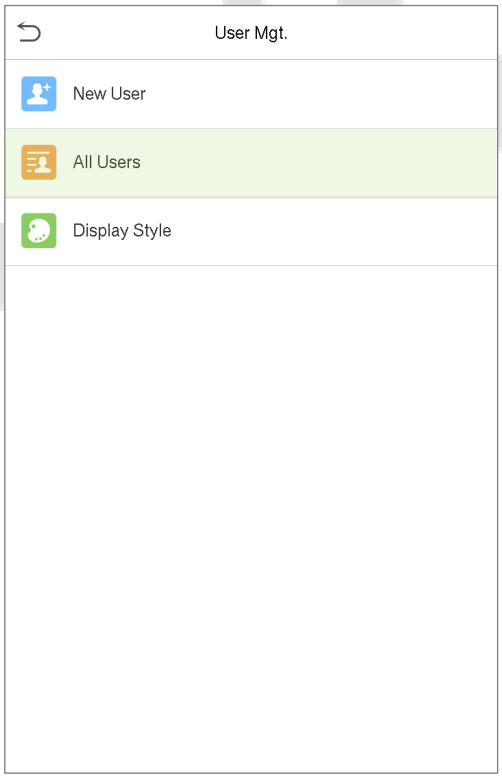
Aplicar período de tiempo de grupo

Sobre el **Control de acceso** interfaz, activar **Aplicar período de tiempo de grupo** para habilitar o deshabilitar el período de tiempo de grupo para cada grupo de acceso.



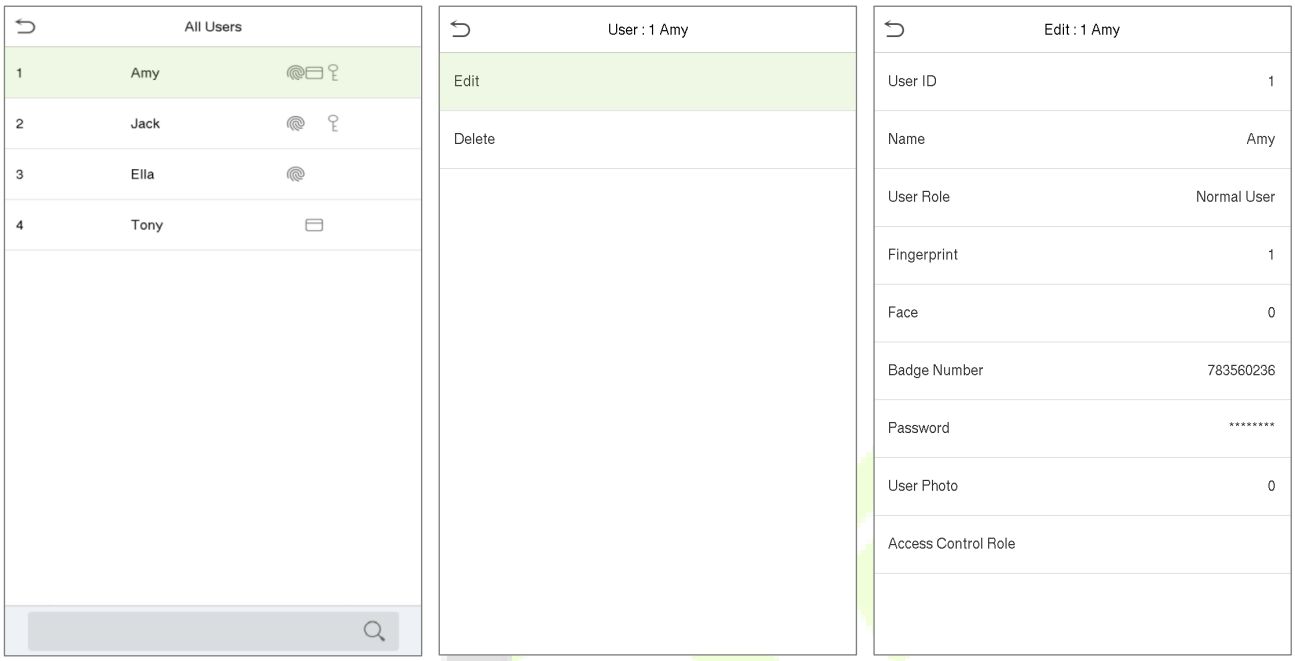
5.2 Buscar usuarios

- Sobre el **Principal** menú, toque **Gestión de usuarios,** y luego toque **Todos los usuarios** para buscar un usuario.
- Sobre el **Todos los usuarios** interfaz, toque en la barra de búsqueda en la lista del usuario para ingresar la palabra clave de recuperación requerida (donde la palabra clave puede ser el ID de usuario, apellido o nombre completo) y el sistema buscará la información de usuario relacionada.



5.3 editar usuario

- En **Todos los usuarios** interfaz, toque el usuario requerido de la lista y toque **Editar** para editar la información del usuario.



Nota: El proceso de editar la información del usuario es el mismo que el de agregar un nuevo usuario, excepto que el ID de usuario no se puede modificar al editar un usuario. Hacer clic aquí para ver el proceso en detalle.

5.4 Borrar usuario

- En **Todos los usuarios** interfaz, toque el usuario requerido de la lista y toque **Eliminar** para eliminar el usuario o la información de un usuario específico del dispositivo.
- Sobre el **Eliminar** interfaz, toque la operación requerida y luego toque OK para confirmar la eliminación.

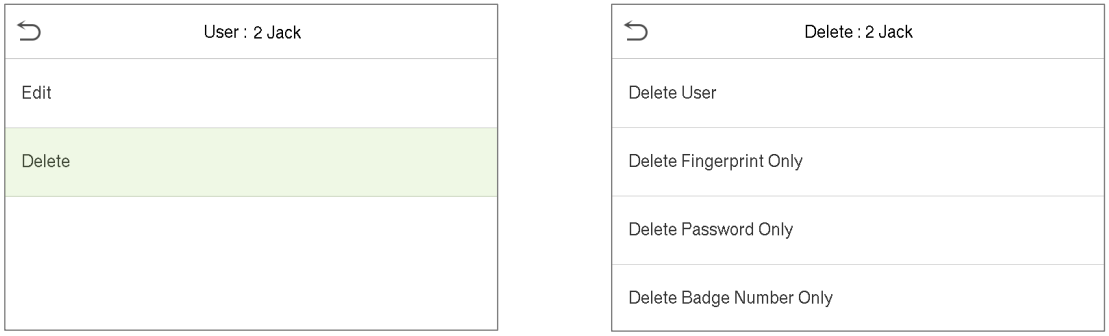
Eliminar operaciones

Borrar usuario: Elimina toda la información del usuario (elimina el usuario seleccionado como un todo) del dispositivo.

Eliminar solo huella digital: Elimina la información de la huella digital del usuario seleccionado.

Eliminar contraseña solamente: Elimina la información de la contraseña del usuario seleccionado.

Eliminar solo el número de tarjeta: Elimina la información del número de tarjeta del usuario seleccionado.

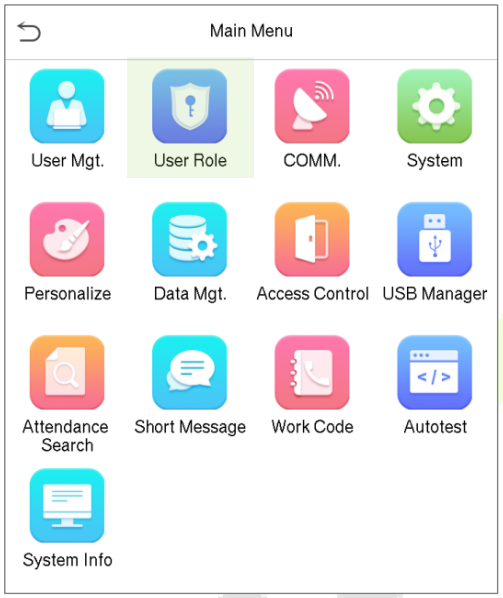


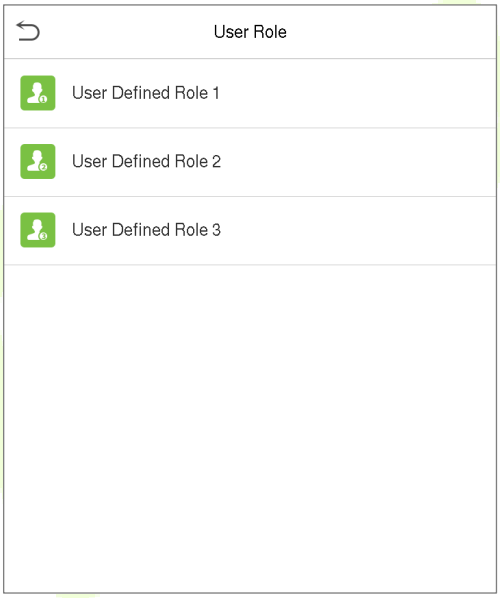
6 Rol del usuario

Rol del usuario facilita la asignación de algunos permisos específicos a determinados usuarios, según el requisito.

- Sobre el **Principal** menú, toque **Rol del usuario,** y luego toque en el **Rol definido por el usuario** para establecer los permisos definidos por el usuario.

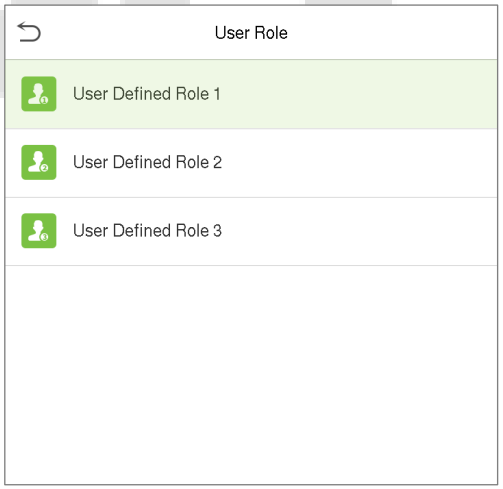
- El alcance del permiso del rol personalizado se puede configurar hasta en 3 roles, es decir, el alcance operativo personalizado de las funciones del menú del usuario.

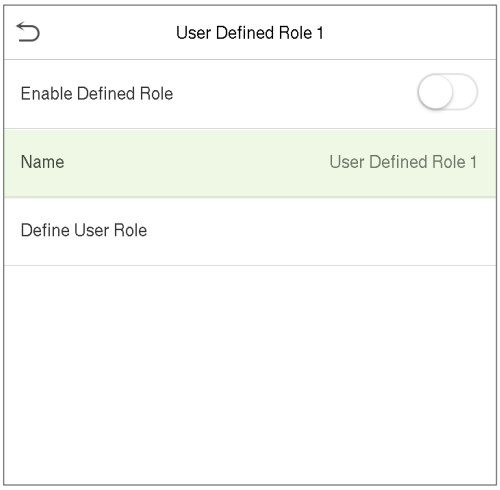




- Sobre el **Rol definido por el usuario** interfaz, alternar **Habilitar rol definido** para habilitar o deshabilitar el rol definido por el usuario.

- Toque en **Nombre** e ingrese el nombre personalizado del rol.

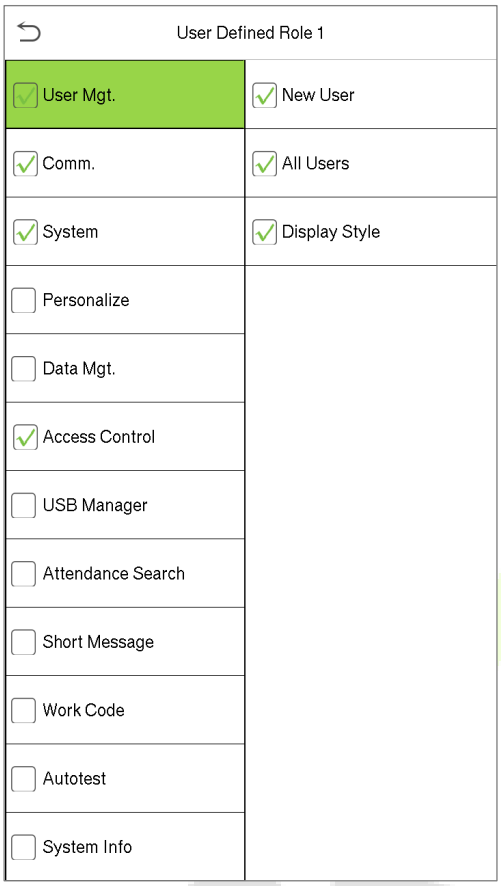


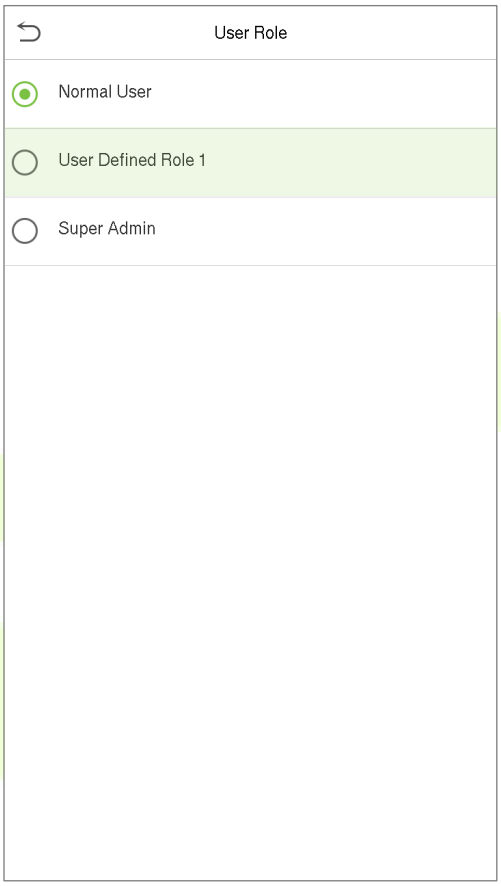


- Luego, toca **Definir rol de usuario** y seleccione los privilegios necesarios para asignar a la nueva función, y luego toque el **Regreso** botón.

- Durante la asignación de privilegios, los nombres de las funciones del menú principal se mostrarán a la izquierda y sus submenús se enumerarán a la derecha.

- Primero toque el nombre de la función requerida del Menú principal y luego seleccione los submenús requeridos de la lista.

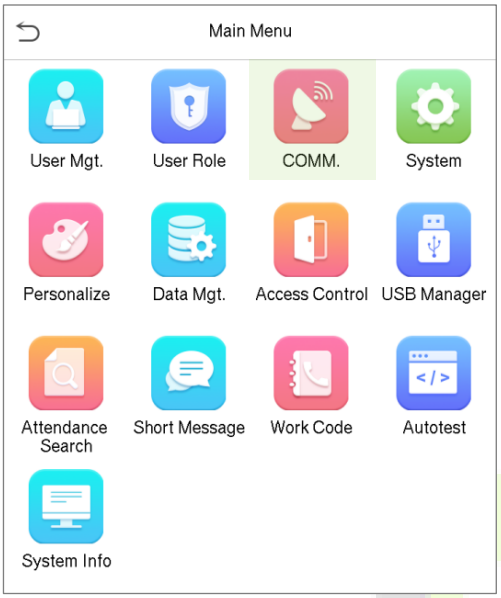


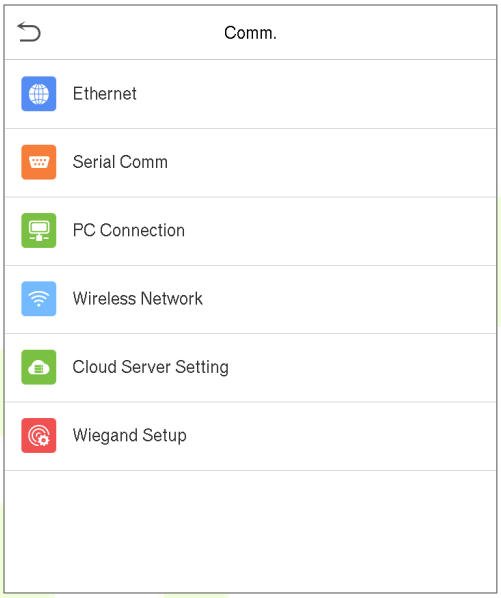


Nota: Si el rol de usuario está habilitado para el dispositivo, toque en **Administrador de usuarios > Nuevo usuario> Rol de usuario** para asignar los roles creados a los usuarios requeridos. Pero si no hay ningún superadministrador registrado en el Dispositivo, el dispositivo le preguntará "¡Inscriba primero al superadministrador!" Al habilitar la función de rol de usuario.

7 Configuración de comunicación

- Sobre el **Menú principal,** grifo **COMM.** para configurar los parámetros de Ethernet, Conexión de PC, Servidor en la nube y Servicio en la nube

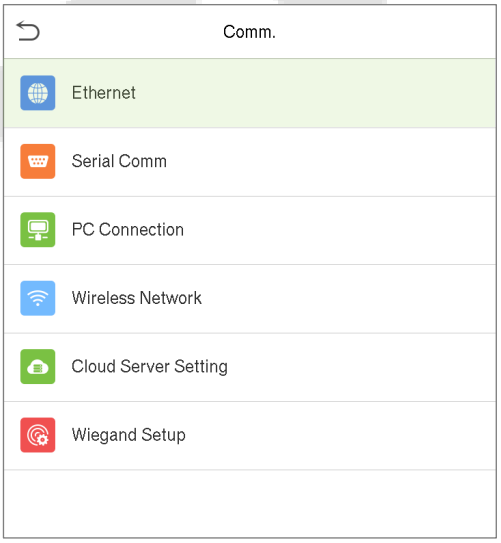


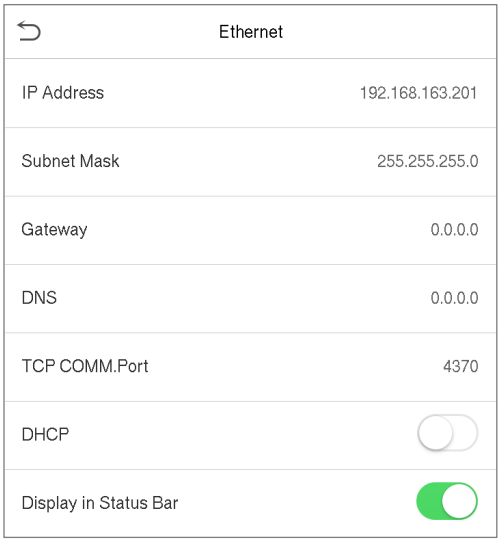


7.1 Configuración de la red

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

- Sobre el **Comm.** Interfaz, toque **Ethernet** para configurar los ajustes.





Función descriptiva

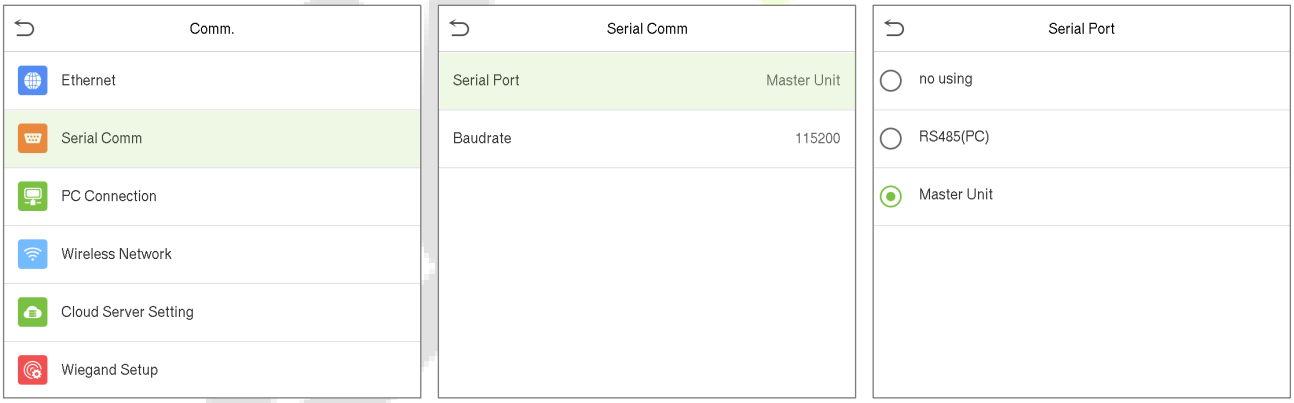
Nombre de la función	Descripción
Dirección IP	La dirección IP predeterminada es 192.168.1.201. Puede modificarse según la disponibilidad de la red.

Máscara de subred	La máscara de subred predeterminada es 255.255.255.0. Puede modificarse según la disponibilidad de la red.
Puerta	La dirección de puerta de enlace predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
DNS	La dirección DNS predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
TCP COMM. Puerto	El valor predeterminado del puerto TCP COMM es 4370. Se puede modificar según la disponibilidad de la red.
DHCP	El Protocolo de configuración dinámica de host consiste en asignar direcciones IP de forma dinámica a los clientes a través del servidor.
Mostrar en la barra de estado Alternar para establecer si se muestra el icono de red en la barra de estado.	

7.2 Comunicaciones en serie

La función de comunicación en serie facilita el establecimiento de comunicación con el dispositivo a través de un número de puerto serie mediante comunicación RS485.

- Sobre el **Comm.** Interfaz, toque **Comunicaciones en serie** para configurar los ajustes del puerto serie.



Función descriptiva

Nombre de la función	Descripción
Puerto serial	**Inhabilitar:** No se comunique con el dispositivo a través del puerto serie. **RS485 (PC):** Se comunica con el dispositivo a través del puerto serie RS485. **Unidad maestra:** Cuando RS485 se utiliza como función de " **Unidad maestra** ", El dispositivo actuará como una unidad maestra y se puede conectar al lector de tarjetas y huellas dactilares RS485.

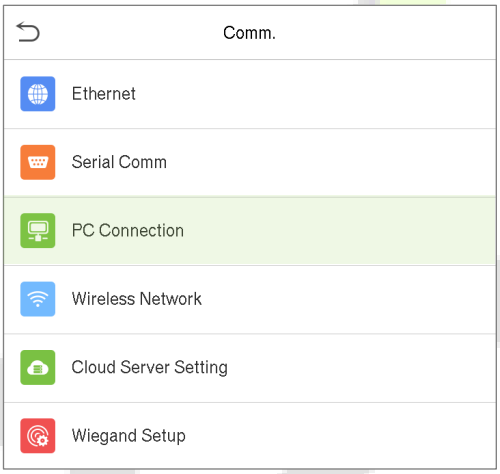
Tasa de baudios	La velocidad a la que se comunican los datos con la PC. Hay 4 opciones de velocidad en baudios: 115200 (predeterminado), 57600, 38400 y 19200. Cuanto mayor es la velocidad en baudios, más rápida es la velocidad de comunicación, pero también menos confiable. Por tanto, se puede utilizar una velocidad en baudios más alta cuando la distancia de comunicación es corta; cuando la distancia de comunicación es larga, elegir una velocidad de transmisión más baja sería más confiable.

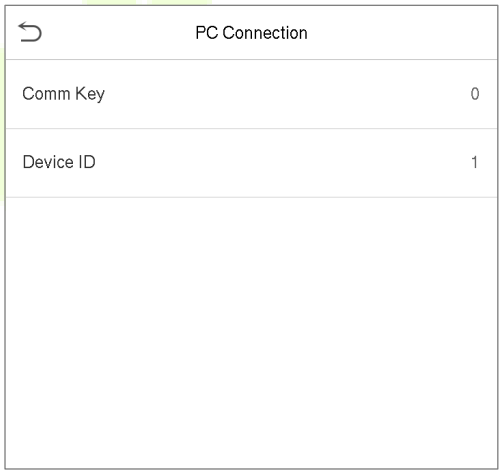
7.3 Conexión a PC

Comm Key facilita mejorar la seguridad de los datos configurando la comunicación entre el dispositivo y la PC.

Una vez configurada la clave de comunicación, se debe proporcionar su contraseña de conexión antes de que el dispositivo se conecte al software de la PC.

- Sobre el **Comm.** Interfaz, toque **Conexión a PC** para configurar los ajustes de comunicación.





Función descriptiva

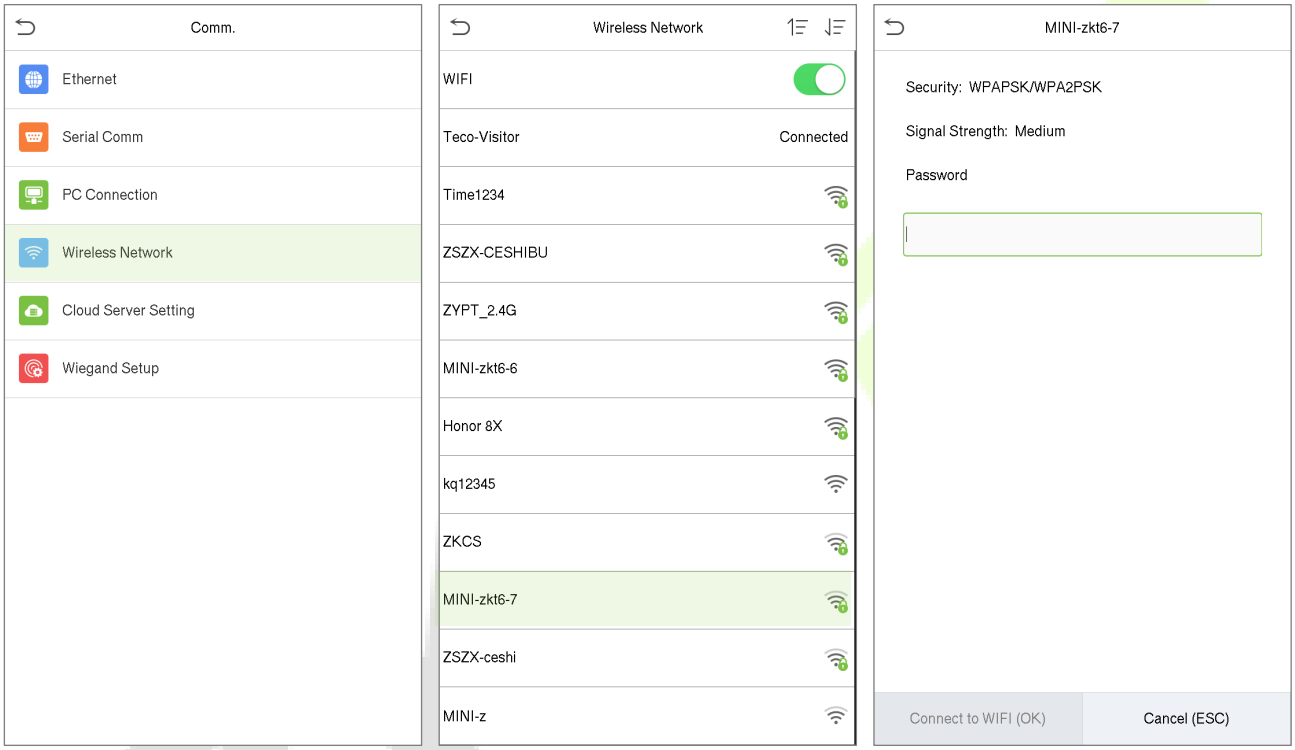
Nombre de la función	Descripciones
CommKey	La contraseña predeterminada es 0 y se puede modificar. La clave de comunicación puede contener de 1 a 6 dígitos.
ID del dispositivo	Número de identidad del dispositivo, que oscila entre 1 y 254. Si el método de comunicación es RS232 / RS485, debe ingresar este ID de dispositivo en la interfaz de comunicación del software.

7.4 Red inalámbrica

El dispositivo proporciona un módulo Wi-Fi, que puede integrarse en el molde del dispositivo o conectarse externamente.

El módulo Wi-Fi permite la transmisión de datos a través de Wi-Fi (Wireless Fidelity) 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 alternar el botón Wi-Fi para deshabilitar.

- Sobre el **Comm.** Interfaz, toque **Red inalámbrica** para configurar los ajustes de WIFI.

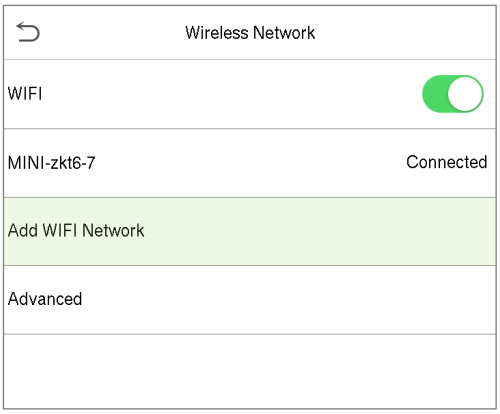


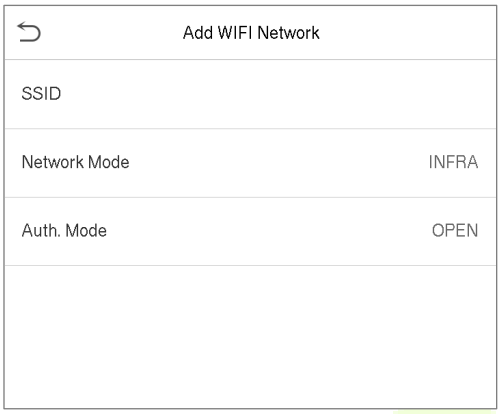
Buscar en la red wifi

- Una vez que el Wi-Fi está encendido, el dispositivo buscará el WIFI disponible dentro del rango de la red.
- Toque el nombre de WiFi apropiado de la lista disponible, ingrese la contraseña correcta en la interfaz de contraseña y luego toque **Conéctese a WIFI (OK).**
- Cuando el WIFI está conectado correctamente, la interfaz inicial mostrará el Wi-Fi logo.

Agregar red WIFI manualmente

- El WIFI también se puede agregar manualmente si el WIFI requerido no se muestra en la lista.
- Sobre el **Red inalámbrica** interfaz, toque en **Agregar red WIFI** para proporcionar los parámetros relevantes (es esencial que la red agregada debe existir).

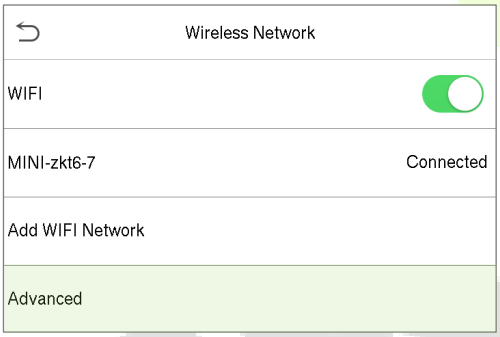


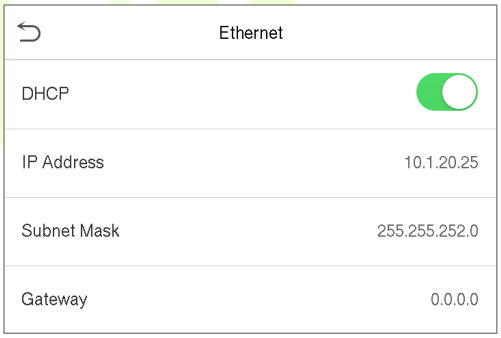


Nota: Después de agregar con éxito el WIFI manualmente, siga el mismo proceso para buscar el nombre WIFI agregado. Hacer clic aquí para ver el proceso de búsqueda de la red WIFI.

Configuración avanzada

- Sobre el **Red inalámbrica** interfaz, toque en **Avanzado** para configurar los parámetros relevantes según sea necesario.





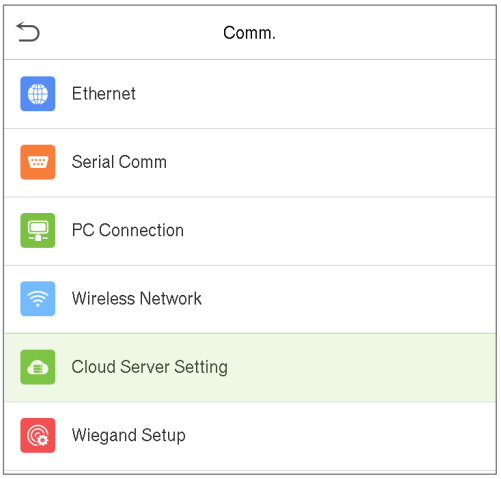
Función descriptiva

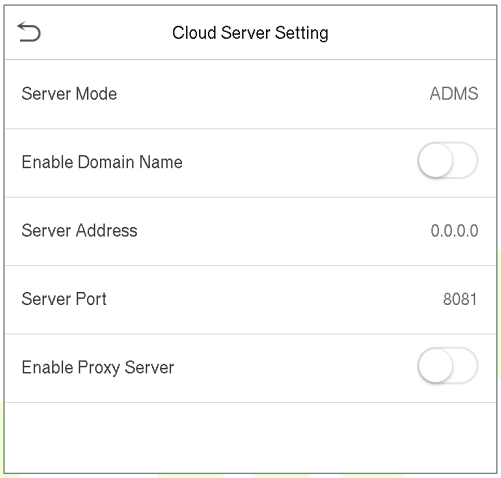
Nombre de la función	Descripciones
DHCP	Protocolo de configuración dinámica de host, que consiste en asignar dinámicamente la dirección IP para los clientes a través del servidor. Si el DHCP está habilitado, la IP no se puede configurar manualmente.
Dirección IP	Dirección IP para la red WIFI, el valor predeterminado es 0.0.0.0. Puede modificarse según la disponibilidad de la red.
Máscara de subred	La máscara de subred predeterminada es 255.255.255.0. Puede modificarse según la disponibilidad de la red.
Puerta	La dirección de puerta de enlace predeterminada es 0.0.0.0. Puede modificarse según la disponibilidad de la red.

Nota: La función WIFI es opcional, solo los productos con el módulo WIFI incorporado están equipados con la función WIFI. Póngase en contacto con nuestro soporte técnico para obtener más información.

7.5 Configuración del servidor en la nube

- Sobre el **Comm.** Interfaz, toque **Configuración del servidor en la nube** para conectarse con el servidor ADMS.



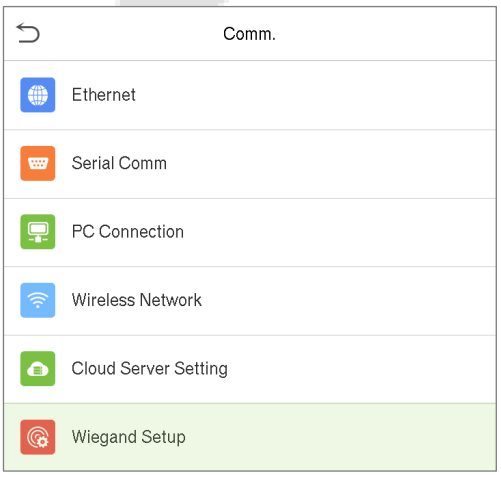


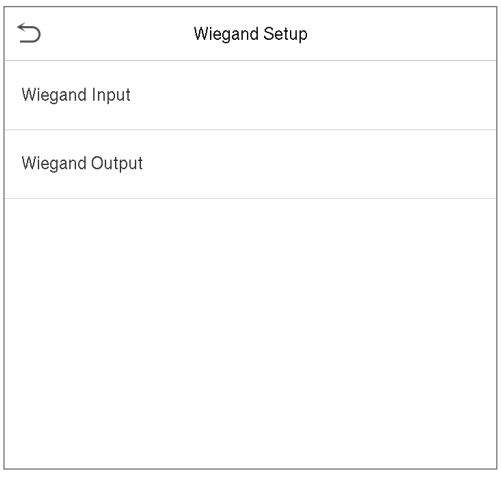
Función descriptiva

Nombre de la función		Descripción
Habilitar dominio Nombre	**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.
Desactivar dominio Nombre	**Dirección del servidor**	Dirección IP del servidor ADMS. Puerto
	Puerto de servicio	utilizado por el servidor ADMS.
Habilitar proxy Servidor		Cuando elige habilitar el proxy, debe configurar la dirección IP y el número de puerto del servidor proxy.

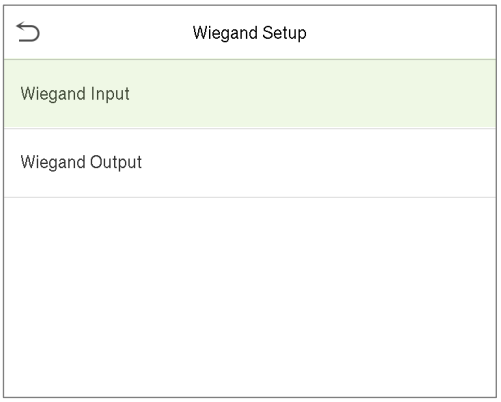
7,6 Configuración de Wiegand

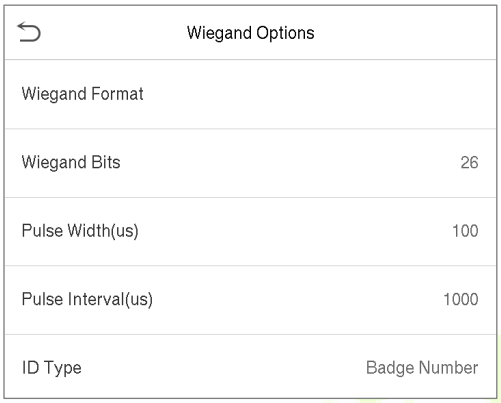
- Sobre el **Comm.** Interfaz, toque **Configuración de Wiegand** para configurar los parámetros de entrada y salida Wiegand.





7.6.1 Entrada Wiegand





Función descriptiva

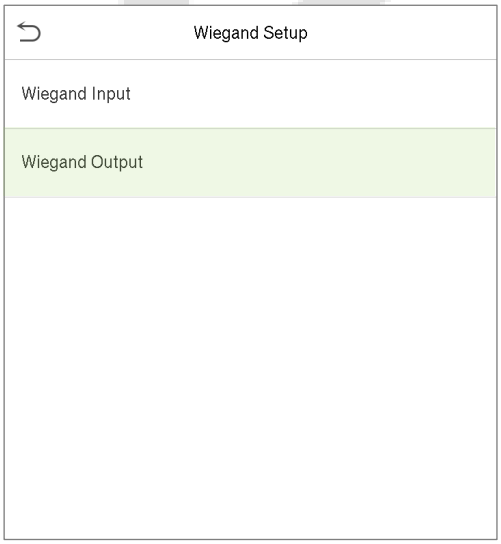
Nombre de la función	Descripciones
Formato Wiegand	El valor varía entre 26 bits, 34 bits, 36 bits, 37 bits y 50 bits. Número de bits
Bits de Wiegand	de WiegandData.
PulseWidth (nosotros)	El valor del ancho de pulso enviado por Wiegand es de 100 microsegundos por defecto y se puede modificar dentro del rango de 20 a 100 microsegundos.
Intervalo de pulso (nosotros)	El valor predeterminado es 1000 microsegundos y se puede modificar dentro del rango de 200 a 20000 microsegundos.
Tipo de identificación	Seleccione el tipo de ID como ID de usuario o Número de tarjeta.

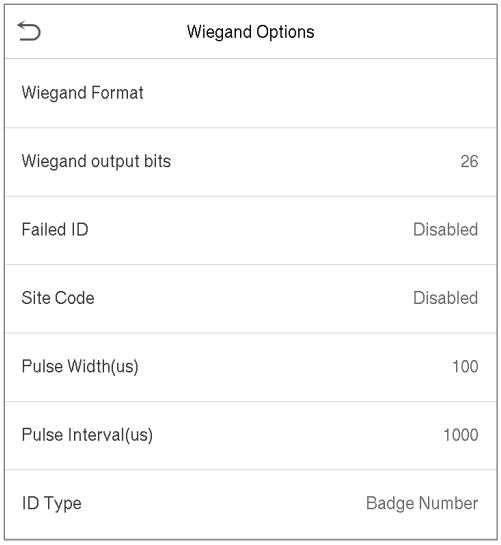
Varias descripciones del formato CommonWiegand:

Formato Wiegand	Descripción
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCC Consta de código binario de 26 bits. El 1 st bit es el bit de paridad par del 2 Dakota del Norte a 13 th bits, mientras que los 26 th bit es el bit de paridad impar del 14 th hasta 25 th bits. 2 Dakota del Norte hasta 25 th los bits son los números de las tarjetas.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCC Consta de 26 bits de código binario. El 1 st bit es el bit de paridad par del 2 Dakota del Norte a 13 th bits, mientras que los 26 th bit es el bit de paridad impar del 14 th hasta 25 th bits. 2 Dakota del Norte al 9 th bits son los códigos de sitio, mientras que los 10 th hasta 25 th los bits son los números de las tarjetas.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Consta de 34 bits de código binario. El 1 st bit es el bit de paridad par del 2 Dakota del Norte hasta 17 th bits, mientras que el 34 th bit es el bit de paridad impar del 18 th hasta 33 rd bits. 2 Dakota del Norte hasta 25 th los bits son los números de las tarjetas.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCC Consta de 34 bits de código binario. El 1 st bit es el bit de paridad par del 2 Dakota del Norte hasta 17 th bits, mientras que el 34 th bit es el bit de paridad impar del 18 th hasta 33 rd bits. 2 Dakota del Norte al 9 th bits son los códigos de sitio, mientras que los 10 th hasta 25 th los bits son los números de las tarjetas.

Wiegand36	APAGADOFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consta de 36 bits de código binario. El 1 s t bit es el bit de paridad impar del 2 Dakota del Norte hasta 18 th bits, mientras que los 36 th bit es el bit de paridad par del 19 th hasta 35 th bits. 2 Dakota del Norte hasta 17 th los bits son los códigos de dispositivo. El 18 th hasta 33 rd los bits son los números de la tarjeta, y los 34 th hasta 35 th los bits son los códigos del fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consta de 36 bits de código binario. El 1 s t bit es el bit de paridad par del 2 Dakota del Norte hasta 18 th bits, mientras que los 36 th bit es el bit de paridad impar del 19 th hasta 35 th bits. 2 Dakota del Norte al 19 th bits son los códigos de dispositivo y los 20 th hasta 35 th los bits son los números de las tarjetas.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCE Consta de 37 bits de código binario. El 1 s t bit es el bit de paridad impar del 2 Dakota del Norte hasta 18 th bits, mientras que el 37 th bit es el bit de paridad par del 19 th hasta 36 th bits. 2 Dakota del Norte para 4 th los bits son los códigos del fabricante. 5 th hasta 16 th bits son los códigos de sitio, y los 21 s t hasta 36 th los bits son los números de las tarjetas.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consta de 37 bits de código binario. El 1 s t bit es el bit de paridad par del 2 Dakota del Norte hasta 18 th bits, mientras que el 37 th bit es el bit de paridad impar del 19 th hasta 36 th bits. 2 Dakota del Norte para 4 th los bits son los códigos del fabricante. 5 th hasta 14 th los bits son los códigos de dispositivo, y 15 th hasta 20 th bits son los códigos de sitio, y los 21 s t hasta 36 th los bits son los números de las tarjetas.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consta de 50 bits de código binario. El 1 s t bit es el bit de paridad par del 2 Dakota del Norte hasta 25 th bits, mientras que los 50 th bit es el bit de paridad impar del 26 th hasta 49 th bits. 2 Dakota del Norte hasta 17 th bits son los códigos de sitio, y los 18 th hasta 49 th los bits son los números de las tarjetas.
"C "Denota el número de tarjeta; " **MI"** denota el bit de paridad par; " **O "** denota el bit de paridad impar; **"F** "Denota el código de la instalación; " **METRO"** denota el código del fabricante; " **PAGS"** denota el bit de paridad; y " **S "** denota el código del sitio.	

7.6.2 Salida Wiegand



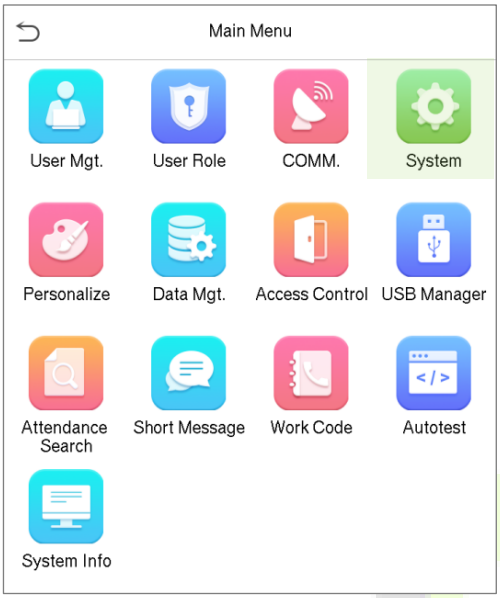


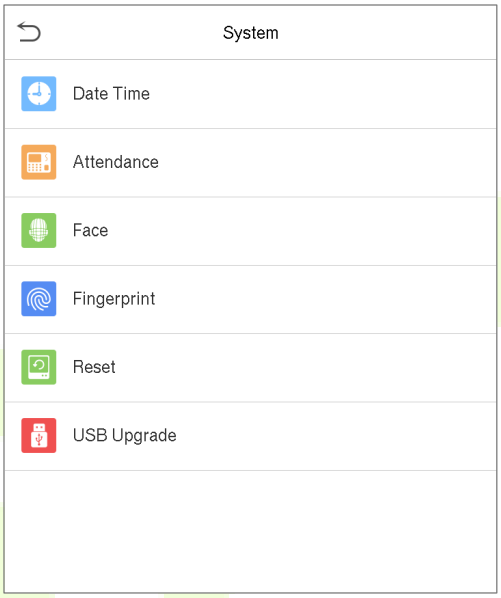
Función descriptiva

Nombre de la función	Descripciones
Formato Wiegand	El valor varía entre 26 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 el ID de personal con el nuevo.
Código del sitio	Es similar al ID del dispositivo. La diferencia es que un código de sitio se puede configurar manualmente y es repetible en cualquier dispositivo. El valor válido varía de 0 a 256 por defecto.
PulseWidth (nosotros)	El ancho de tiempo representa el cambio en la cantidad de carga eléctrica con capacitancia regular de alta frecuencia dentro del tiempo especificado.
Intervalo de pulso (nosotros)	El intervalo de tiempo entre pulsos.
Tipo de identificación	Seleccione el tipo de ID como ID de usuario o Número de tarjeta.

8 Ajustes del sistema

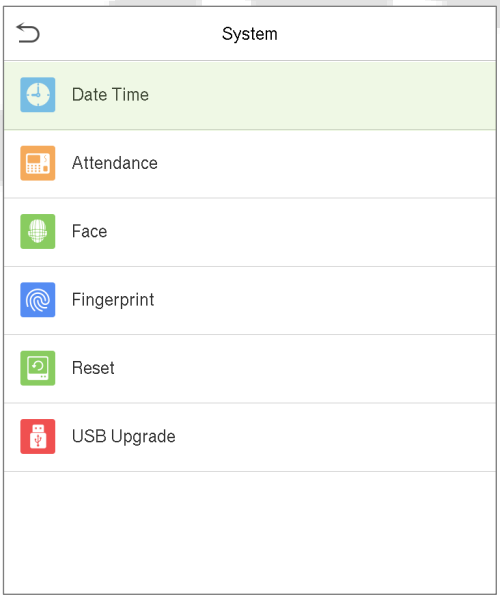
- Sobre el **Menú principal,** grifo **Sistema** para configurar los parámetros del sistema relacionados con el fin de optimizar el rendimiento del dispositivo.

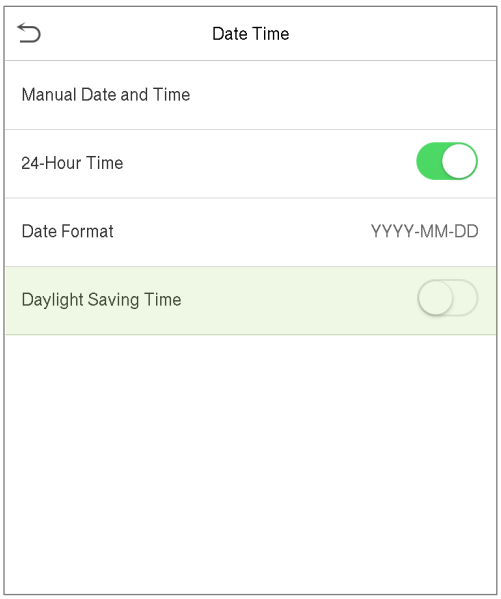




8.1 Fecha y hora

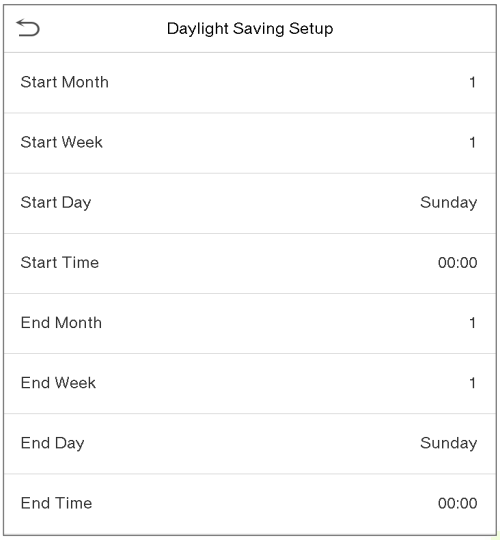
- Sobre el **Sistema** Interfaz, toque **Fecha y hora** para configurar la fecha y la hora.



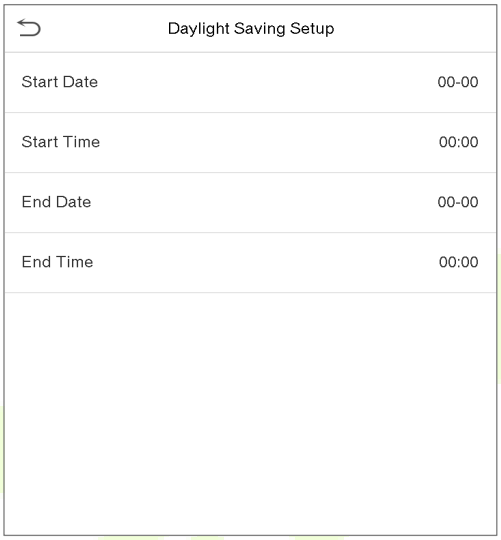


- Grifo **Fecha y hora manuales** para configurar manualmente la fecha y la hora y toque **Confirmar** ahorrar.
- Grifo **24 horas** para habilitar o deshabilitar este formato. Si está habilitado, toque **Formato de fecha** para configurar el formato de fecha.

- ★ Grifo **Horario de verano** para habilitar o deshabilitar la función. Si está habilitado, toque **Modo de ahorro de luz diurna** para seleccionar un modo de horario de verano y luego toque **Configuración de horario de verano** para configurar la hora del cambio.



Modo semana



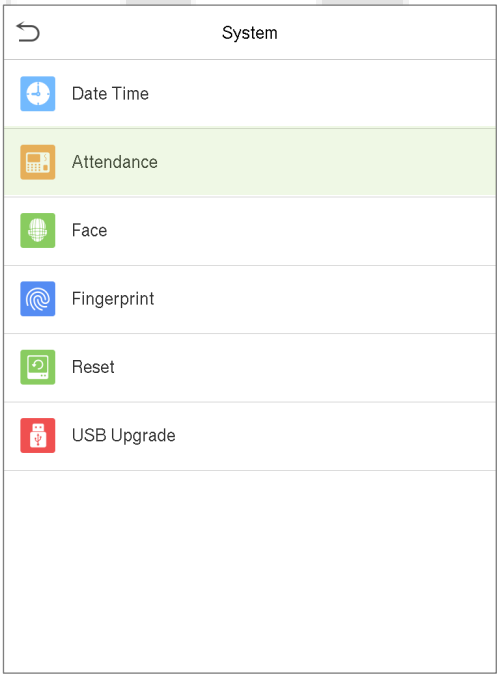
Modo de fecha

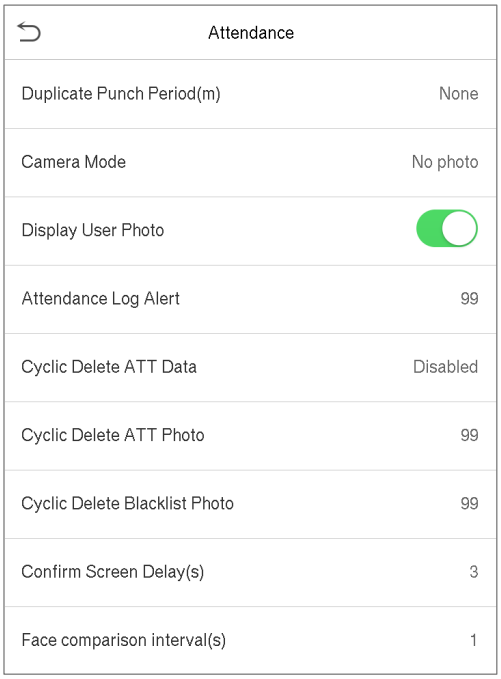
- Al restaurar la configuración de fábrica, la hora (24 horas) y el formato de fecha (AAAA-MM-DD) se pueden restaurar, pero la fecha y la hora del dispositivo no se pueden restaurar.

Nota: Por ejemplo, el usuario establece la hora del dispositivo (18:35 del 15 de marzo de 2019) a las 18:30 de enero 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, 2020.

8.2 Configuración de registros de asistencia / acceso

- Sobre el **Sistema** interfaz, toque **Asistencia** para ir a la configuración de acceso o registro de asistencia.



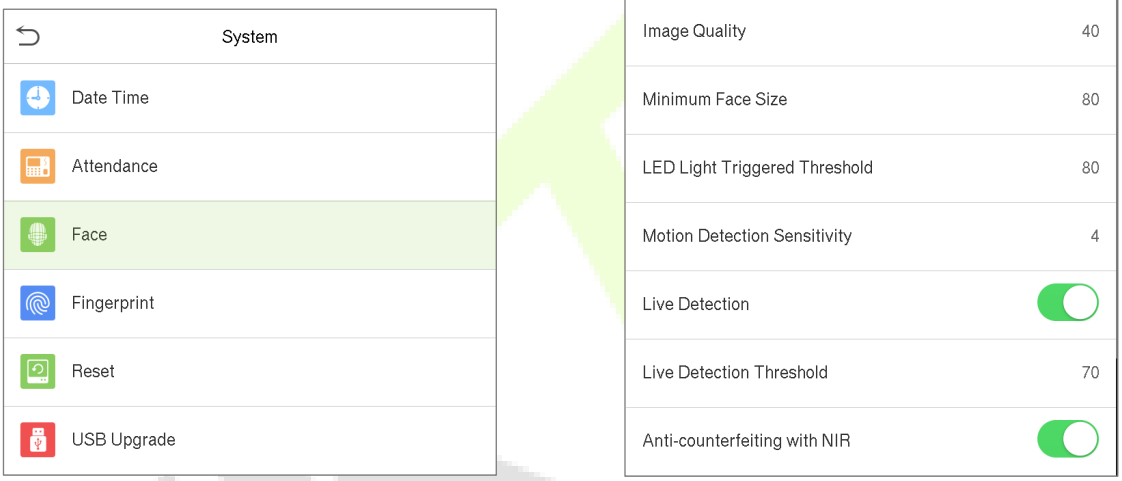


Función descriptiva

Nombre de la función	Descripción
Período de perforación duplicado (metro)	Una vez que se establece el rango de tiempo, el registro de asistencia de la misma persona no se guardará; el valor válido varía de 1 a 999999 minutos.
Modo cámara	Ya sea para capturar y guardar la imagen instantánea actual durante la verificación. Hay 5 modos: **Sin fotografía:** No se tomará ninguna foto durante la verificación del usuario. **Tomar una foto, no guardar:** Se tomará una foto, pero no se guardará durante la verificación. **Tomar una foto y guardar:** La foto se tomará y guardará durante la verificación. **Ahorre en la verificación exitosa:** La foto se tomará y guardará solo para cada verificación exitosa. **Guardar en verificación fallida:** La foto se tomará y guardará solo por cada verificación fallida.
Mostrar foto de usuario	Si mostrar la foto del usuario cuando el usuario pasa la verificación.
Alerta de registro de asistencia / Registros de acceso	Cuando el espacio de registro del registro de asistencia / registro de acceso alcanza el valor de umbral máximo, el dispositivo mostrará automáticamente la advertencia de espacio de memoria. Puede borrar los registros o desactivar la función o establecer un valor válido entre 1 y 9999.
Eliminación cíclica ATT Registros de datos / acceso	Cuando los registros de asistencia / acceso hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de registros de asistencia / acceso antiguos. Puede desactivar la función o establecer un valor válido entre 1 y 999.
Eliminación cíclica de foto ATT	Cuando las fotos de asistencia hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos de asistencia antiguas. Puede desactivar la función o establecer un valor válido entre 1 y 99.
Lista negra de eliminación cíclica Foto	Cuando las fotos de la lista negra hayan alcanzado su capacidad máxima, el dispositivo eliminará automáticamente un conjunto de fotos antiguas de la lista negra. Puede desactivar la función o establecer un valor válido entre 1 y 99.
Confirmar retraso de pantalla	El tiempo que muestra el mensaje de verificación exitosa. Valor válido: 1 ~ 9 segundos.
Intervalo (s) de detección de rostro	Establece el intervalo de tiempo de coincidencia de la plantilla facial según sea necesario. Valor válido: 0 ~ 9 segundos.

8.3 Parámetros faciales

- Sobre el **Sistema** interfaz, toque **Cara** para ir a la configuración de los parámetros de la cara.



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

Función descriptiva

Nombre de la función	Descripción
1: NThresholdValue	En el modo de verificación 1: N, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas sea mayor que el valor establecido. El valor válido varía entre 65 y 120. Cuanto mayor sea el umbral, menor será la tasa de errores de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 75.

1: 1ThresholdValue	En el modo de verificación 1: 1, la verificación solo tendrá éxito cuando la similitud entre la imagen facial adquirida y las plantillas faciales del usuario registradas en el dispositivo sea mayor que el valor establecido. El valor válido varía de 55 a 120. Cuanto más altos sean los umbrales, menor será la tasa de errores de juicio, mayor será la tasa de rechazo y viceversa. Se recomienda establecer el valor predeterminado de 63.
Inscripción Valor umbral	Durante el registro facial, se utiliza la comparación 1: N para determinar si el usuario ya se ha registrado antes. Cuando la similitud entre la imagen facial adquirida y todas las plantillas faciales registradas es mayor que este valor umbral, indica que la cara ya ha sido registrada.
Ángulo de inclinación de la cara	La tolerancia del ángulo de inclinación de una cara para el registro facial y la comparación. Si el ángulo de inclinación de una cara excede este valor establecido, el algoritmo lo filtrará, es decir, ignorado por el terminal, por lo que no se activará ninguna interfaz de registro y comparación.
Rotación facial Ángulo	La tolerancia del ángulo de rotación de una cara para el registro y la comparación de plantillas faciales. Si el ángulo de rotación de una cara excede este valor establecido, será filtrado por el algoritmo, es decir, ignorado por el terminal, por lo que no se activará ninguna interfaz de registro y comparación.
Calidad de la imagen	Calidad de imagen para registro facial y comparación. Cuanto mayor sea el valor, más clara será la imagen requerida.
Mínimo Reconocimiento Valor	Requerido para el registro facial y la comparación. Si el tamaño mínimo de la figura capturada es menor que este valor establecido, se filtrará y no se reconocerá como una cara. Este valor puede entenderse como la distancia de comparación de caras. Cuanto más lejos esté la persona, más pequeña será la cara y el algoritmo obtendrá el píxel de la cara más pequeño. Por lo tanto, ajustar este parámetro puede ajustar la distancia de comparación más lejana de caras. Cuando el valor se establece en 0, la distancia de comparación de caras no está limitada.
Disparador de luz LED Valor	Este valor controla el encendido y apagado de la luz LED. Cuanto mayor sea el valor, con más frecuencia se encenderá la luz LED.
Detección de movimiento Sensibilidad	Es para establecer el valor de la cantidad de cambio en el campo de visión de la cámara, que se conoce como valor de detección de movimiento potencial, que despierta el terminal desde el modo de espera a la interfaz de comparación. Cuanto mayor sea el valor, más sensible será el sistema, es decir, si se establece un valor mayor, la interfaz de comparación es mucho más fácil y la detección de movimiento se activa con frecuencia.
Detección en vivo	Detectar el intento de falsificación utilizando imágenes de luz visible para determinar si la muestra de fuente biométrica proporcionada es realmente una persona (un ser humano vivo) o una representación falsa.
Detección en vivo ThresholdValue	Facilita juzgar si la imagen visible capturada es realmente una persona (un ser humano vivo). Cuanto mayor sea el valor, mejor será el rendimiento anti-spoofing con luz visible.

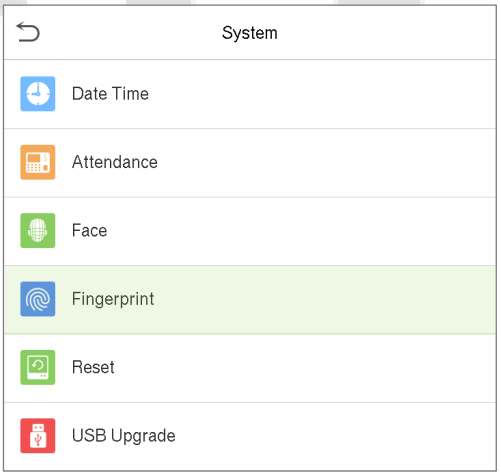
Anti-spoofing usando NIR	Utiliza imágenes de espectros de infrarrojo cercano para identificar y prevenir fotos falsas y ataques de video.
WDR	Amplio rango dinámico (WDR), que equilibra la luz y extiende la visibilidad de la imagen para videos de vigilancia en escenas de iluminación de alto contraste y mejora la identificación de objetos en ambientes brillantes y oscuros.
Modo anti-parpadeo	Se utiliza cuando WDR está desactivado. Esto ayuda a reducir el parpadeo cuando la pantalla del dispositivo parpadea a la misma frecuencia que la luz.
Notas	Un ajuste inadecuado de los parámetros de exposición y calidad puede afectar gravemente el rendimiento del dispositivo. Ajuste el parámetro de exposición solo bajo la guía del personal de servicio postventa de nuestra empresa.

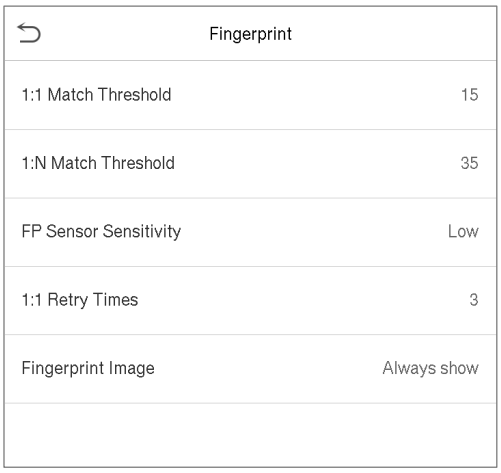
Proceso para modificar la precisión del reconocimiento facial

- Sobre el **Sistema** interfaz, toque en **Cara** y luego alternar para habilitar Anti-Spoofing usando NIR para configurar el Anti-Spoofing.
- Entonces, en el **Menú principal,** grifo **Prueba automática> Cara de prueba** y realice la prueba facial.
- Toque tres veces para ver las puntuaciones en la esquina superior derecha de la pantalla y aparecerá el cuadro rectangular rojo para comenzar a ajustar el modo.
- Mantenga la distancia de un brazo entre el dispositivo y la cara, y se recomienda no mover la cara en un rango amplio.

8.4 Parámetros de huellas dactilares

- Sobre el **Sistema** interfaz, toque **Huella dactilar** para configurar los ajustes de la huella digital.





FRR	LEJOS	Umbrales de coincidencia recomendados	
		1: N	1: 1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Alto	25	10

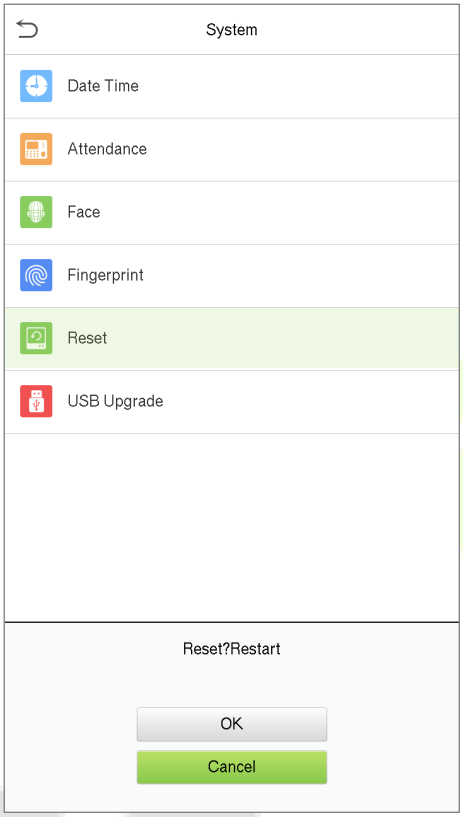
Función descriptiva

Nombre de la función	Descripciones
1: 1 Umbral	En el método de verificación 1: 1, la verificación solo tendrá éxito cuando la similitud entre los datos de huellas dactilares adquiridos y la plantilla de huellas dactilares asociada con la ID de usuario ingresada que está inscrita en el dispositivo es mayor que el valor establecido.
1: N umbral	En el método de verificación 1: N, la verificación solo tendrá éxito 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 establecer la sensibilidad de la adquisición de huellas dactilares. Se recomienda utilizar el nivel predeterminado " **Medio".** Cuando el ambiente está seco, lo que resulta en una detección lenta de huellas dactilares, puede establecer el nivel en " **Alto"** elevar la sensibilidad; cuando el ambiente es húmedo, lo que dificulta la identificación de la huella digital, puede establecer el nivel en " **Bajo** ".
Intentos de reintento 1: 1	Los usuarios pueden olvidar la huella digital registrada o presionar el dedo de manera incorrecta. La Verificación 1: 1 permite configurar los intentos de reintento de autenticación para los usuarios con el fin de reducir el proceso de volver a ingresar el ID de usuario y aumentar la seguridad.
Imagen de huella digital	Para configurar si se muestra la imagen de la huella digital en la pantalla durante el registro o la verificación de la huella digital. 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. • **Siempre muestra:** para mostrar la imagen de la huella digital en la pantalla durante el registro y la verificación. • **Ninguna:** no mostrar la imagen de la huella digital.

8.5 Restablecimiento de fábrica

La función Factory Reset 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 de usuario registrados).

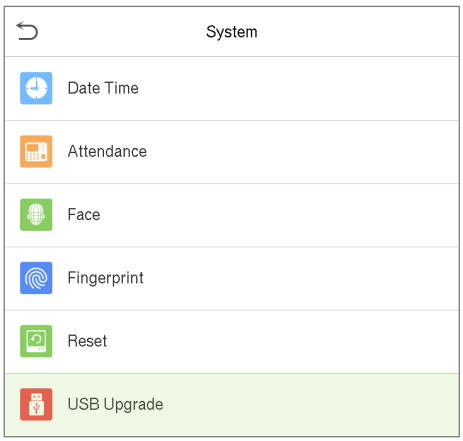
- Sobre el **Sistema** interfaz, toque **Reiniciar** y luego toque **Okay** para restaurar la configuración predeterminada de fábrica.



8,6 Actualización USB

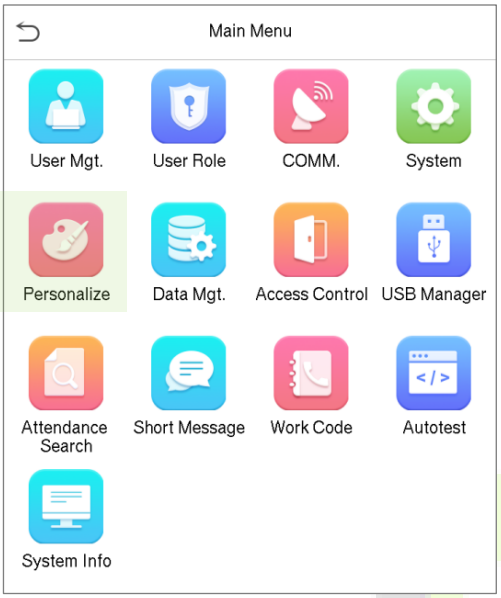
El programa de firmware del dispositivo se puede actualizar con el archivo de actualización en una unidad USB. Antes de realizar esta operación, asegúrese de que la unidad USB contenga el archivo de actualización correcto y esté correctamente insertada en el dispositivo.

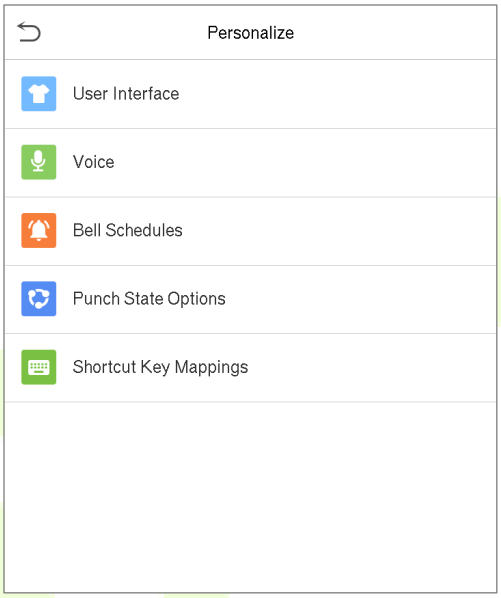
- Sobre el **Sistema** interfaz, toque **Actualización USB** para actualizar el firmware del dispositivo.



9 Personalizar la configuración

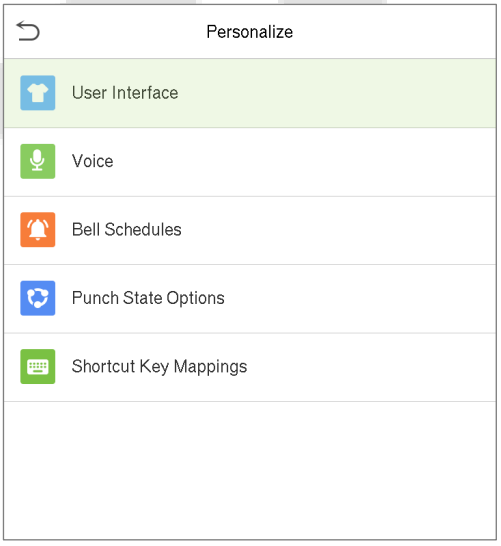
- Sobre el **Menú principal,** grifo **Personalizar** personalizar la configuración de la interfaz, voz, timbre, opciones de estado de perforación y asignaciones de teclas de acceso directo ★.

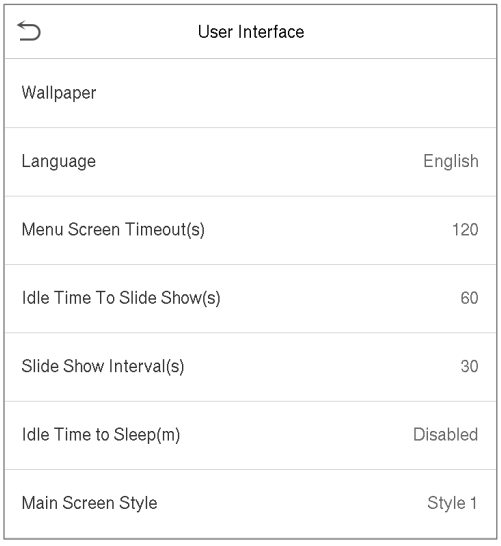




9.1 Configuración de la interfaz

- Sobre el **Personalizar** interfaz, toque **Interfaz de usuario** para personalizar el estilo de visualización de la interfaz principal.





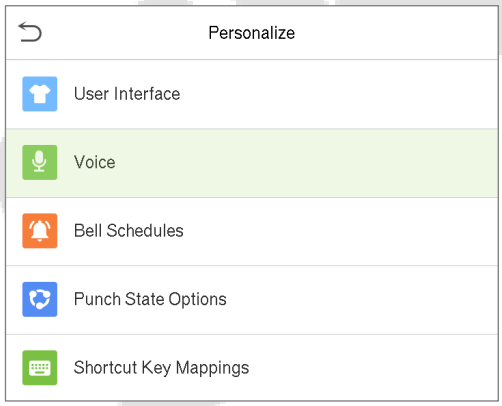
Función descriptiva

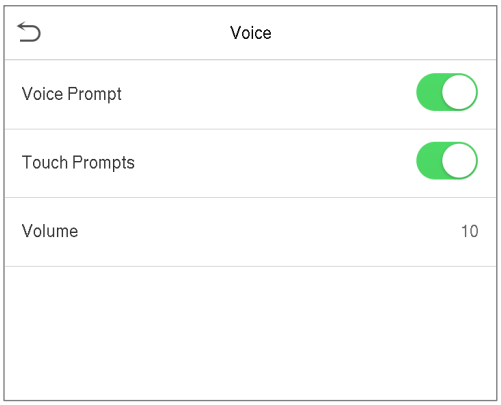
Nombre de la función	Descripción
Fondo de pantalla	El fondo de pantalla de la pantalla principal se puede seleccionar de acuerdo con las preferencias del usuario.

Idioma	Seleccione el idioma del dispositivo.
Pantalla de menú Tiempo de espera (s)	Cuando no hay operación y el tiempo excede el valor establecido, el dispositivo volverá automáticamente a la interfaz inicial. Esta función puede deshabilitarse o establecer el valor requerido entre 60 y 99999 segundos.
Tiempo de inactividad para deslizar Mostrar (s)	Cuando no hay ninguna operación y el tiempo excede el valor establecido, se reproducirá una presentación de diapositivas. Esta función se puede desactivar o establecer el valor requerido entre 3 y 999 segundos.
Intervalo de presentación de diapositivas (s)	Es un intervalo de tiempo para cambiar entre diferentes imágenes como un proceso de presentación de diapositivas. La función se puede desactivar o establecer el intervalo de tiempo requerido entre 3 y 999 segundos.
Tiempo inactivo para dormir (metro)	Si el modo de suspensión está activado y cuando no hay ninguna operación en el dispositivo, el dispositivo pasará al modo de espera. Presione cualquier tecla o dedo para reanudar el modo de trabajo normal. Esta función se puede desactivar o establecer un valor dentro de 1-999 minutos.
Estilo de pantalla principal	El estilo de la pantalla principal se puede seleccionar según las preferencias del usuario.

9.2 Configuración de voz

- Sobre el **Personalizar** interfaz, toque **Voz** para configurar los ajustes de voz.



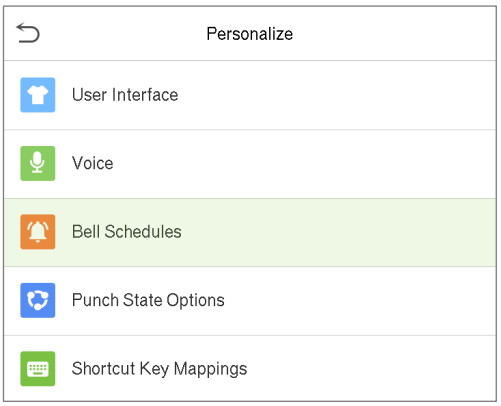


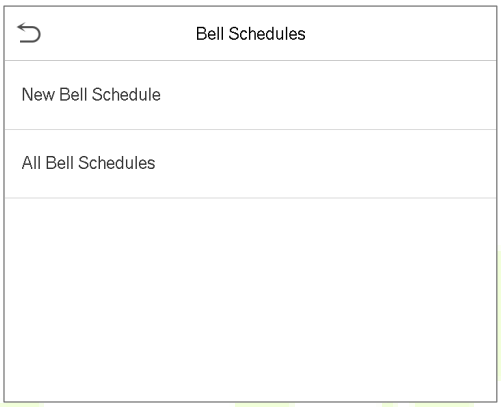
Función descriptiva

Nombre de la función	Descripción
Mensaje de voz	Cambie para habilitar o deshabilitar las indicaciones de voz durante las operaciones de la función. Cambie para
Toque Indicación	habilitar o deshabilitar los sonidos del teclado.
Volumen	Ajusta el volumen del dispositivo y se puede establecer entre: 0-100.

9.3 Horarios de campana

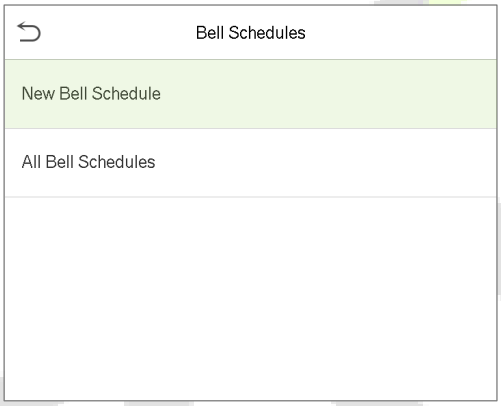
- Sobre el **Personalizar** interfaz, toque **Horarios de campana** para configurar los ajustes de la campana.

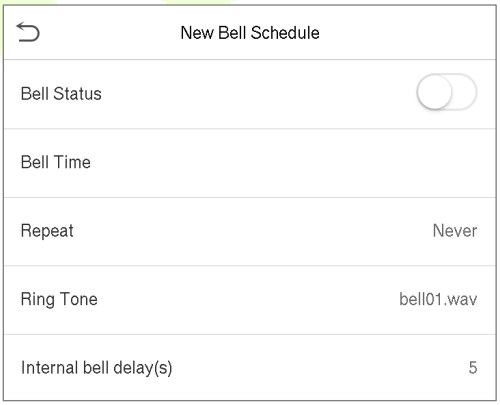




Horario NewBell

- Sobre el **Horarios de campana** interfaz, toque **Horario NewBell** para agregar un nuevo horario de timbre.





Función descriptiva

Nombre de la función	Descripción
Estado de la campana	Cambie para habilitar o deshabilitar el estado de la campana.
Tiempo de campana	Una vez que se establece el tiempo requerido, el dispositivo se activará automáticamente para hacer sonar la campana durante ese tiempo.
Repetir	Configure el número requerido de conteos para repetir la campana programada.
Tono de llamada	Seleccione un tono de llamada.
Repetir retardo de campana (s)	Establece el tiempo de repetición de la campana programada. Los valores válidos oscilan entre 1 y 999 segundos.

Todos los horarios de campana

- Una vez programada la campana, el **Horarios de campana** interfaz, toque **Todos los horarios de campana** para ver la campana recién programada.

Editar la campana programada

- Sobre el **Todos los horarios de campana** interfaz, toque el horario de timbre requerido y toque **Editar** para editar el horario de timbre seleccionado.

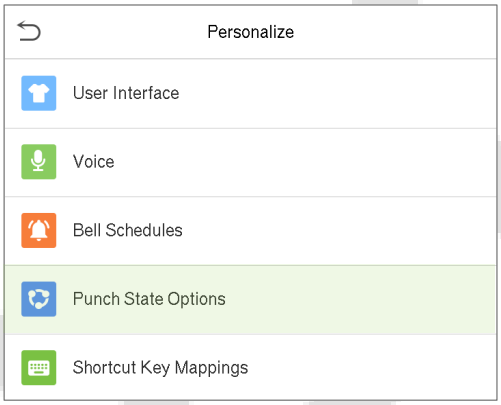
- El método de edición es el mismo que el de agregar un nuevo horario de campana.

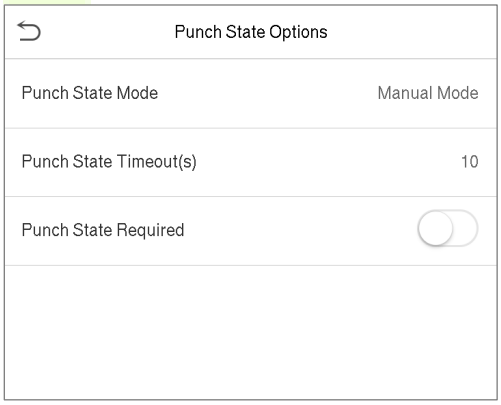
Eliminar una campana

- En la interfaz de Todos los horarios de timbre, toque el horario de timbre requerido y toque **Eliminar,** y luego toque **si** para eliminar la campana seleccionada.

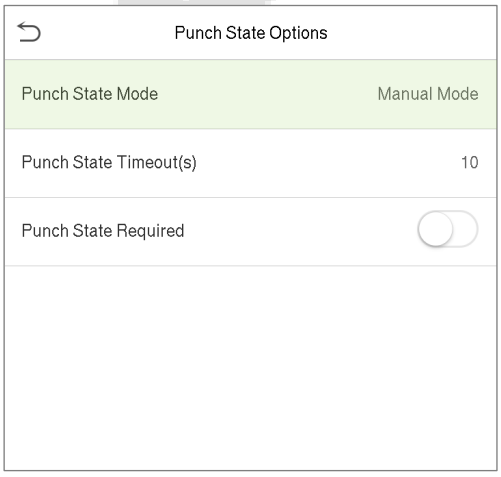
9.4 Opciones de estado de perforación

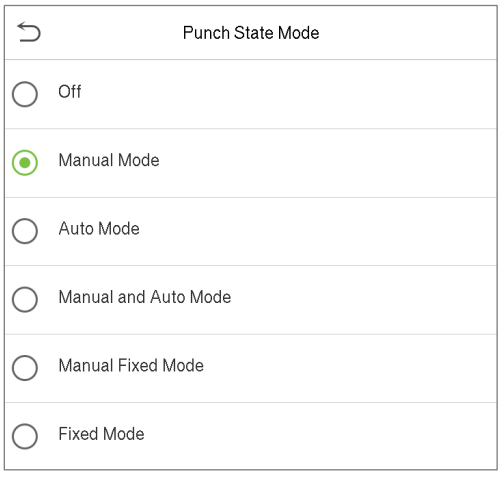
- Sobre el **Personalizar** interfaz, toque **Opciones de estado de perforación** para configurar los ajustes del estado de perforación.





Modo de estado de perforación





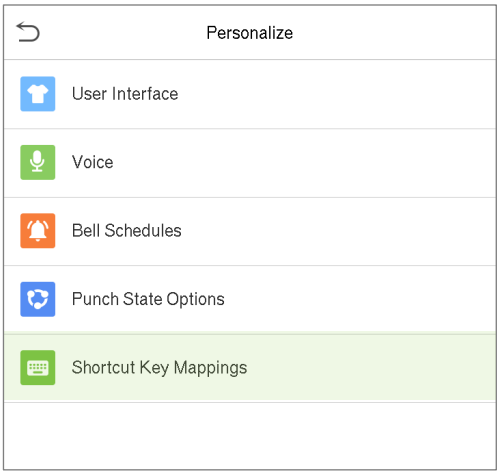
Función descriptiva

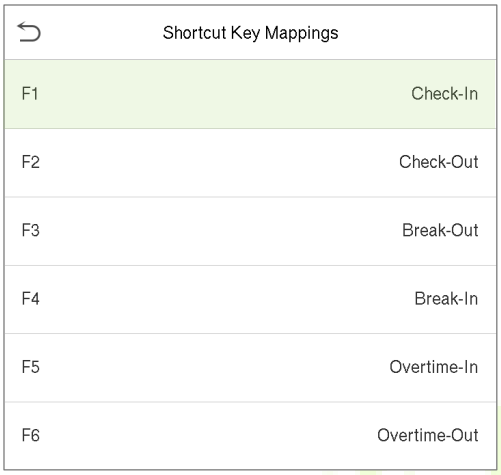
Articulo	Descripción
Modo de estado de perforación	**Apagado:** Desactiva la función de estado de perforación. Por lo tanto, la tecla de estado de perforación configurada en el menú Asignaciones de teclas de acceso directo no funcionará. **Modo manual:** Cambia la tecla de estado de perforación manualmente; el estado de asistencia se restablecerá automáticamente después del tiempo de espera. **Modo automático:** La tecla de estado de marcado cambiará automáticamente a un estado de marcado específico de acuerdo con el horario predefinido que se puede configurar en las asignaciones de teclas de acceso directo. **Modo manual y automático:** La interfaz principal mostrará la tecla de estado de perforación de cambio automático. Sin embargo, los usuarios aún podrán seleccionar una alternativa que sea el estado de asistencia manual. Después del tiempo de espera, la tecla de estado de perforación de conmutación manual se convertirá en la tecla de estado de perforación de conmutación automática. **Modo fijo manual:** Después de que la tecla de estado de perforación se configure manualmente a un estado de perforación particular, la función permanecerá sin cambios hasta que se cambie manualmente nuevamente. **Modo fijo:** Solo se mostrará la clave de estado de perforación fijada manualmente. Los usuarios no pueden cambiar el estado presionando otras teclas.
Tiempo de espera de estado de	La duración del tiempo de espera, es decir, permanecer inactivo en el menú principal.
perforación Estado de perforación requerido	Para establecer si se debe seleccionar el estado de asistencia durante la verificación.

9.5 Asignaciones de teclas de método abreviado

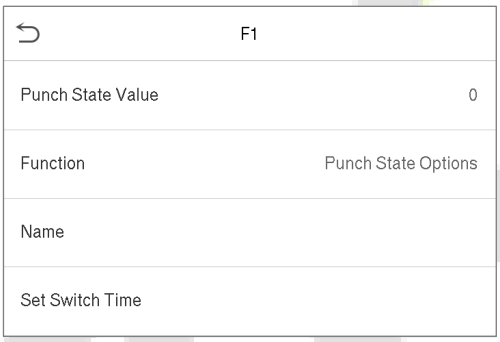
Los usuarios pueden definir teclas de acceso directo para el estado de asistencia y para las teclas funcionales que se definirán en la interfaz principal. Por lo tanto, en la interfaz principal, cuando se presionan las teclas de acceso directo, el estado de asistencia correspondiente o la interfaz de función se mostrará directamente.

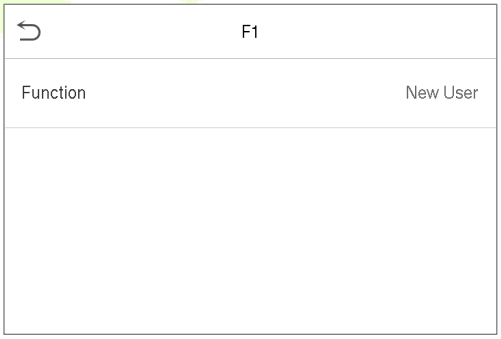
- Sobre el **Personalizar** interfaz, toque **Asignaciones de teclas de método abreviado** para configurar las teclas de método abreviado necesarias.





- Sobre el **Asignaciones de teclas de método abreviado** interfaz, toque la tecla de acceso directo requerida para configurar los ajustes de la tecla de acceso directo.
- Sobre el **Tecla de acceso directo (** que es "F1"), toque **función** para configurar el proceso funcional de la tecla de método abreviado como tecla de estado de perforación o tecla de función.
- Si la tecla de acceso directo se define como una tecla de función (como Nuevo usuario, Todos los usuarios, etc.), la configuración se completa como se muestra en la imagen siguiente.

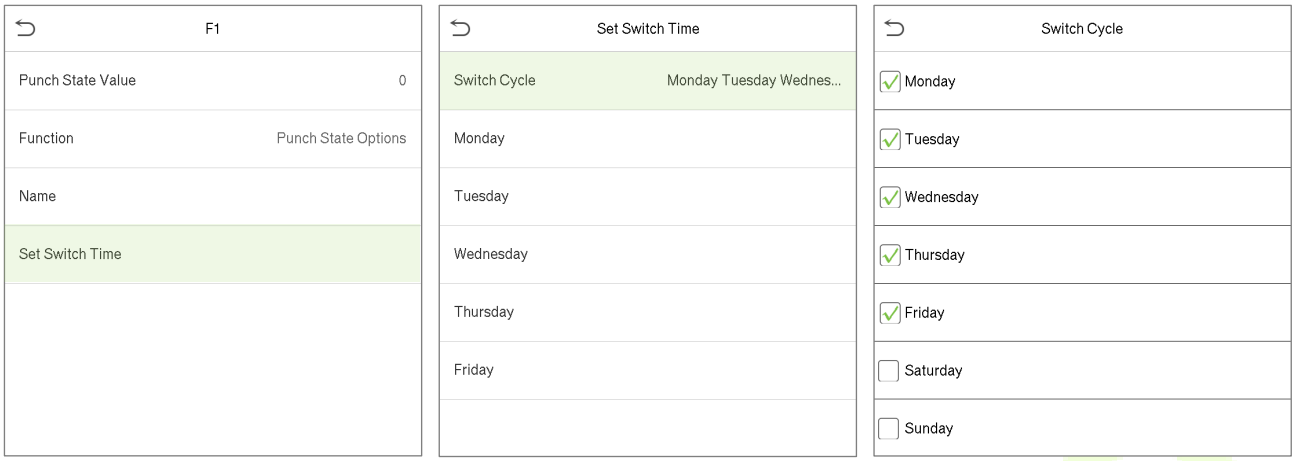




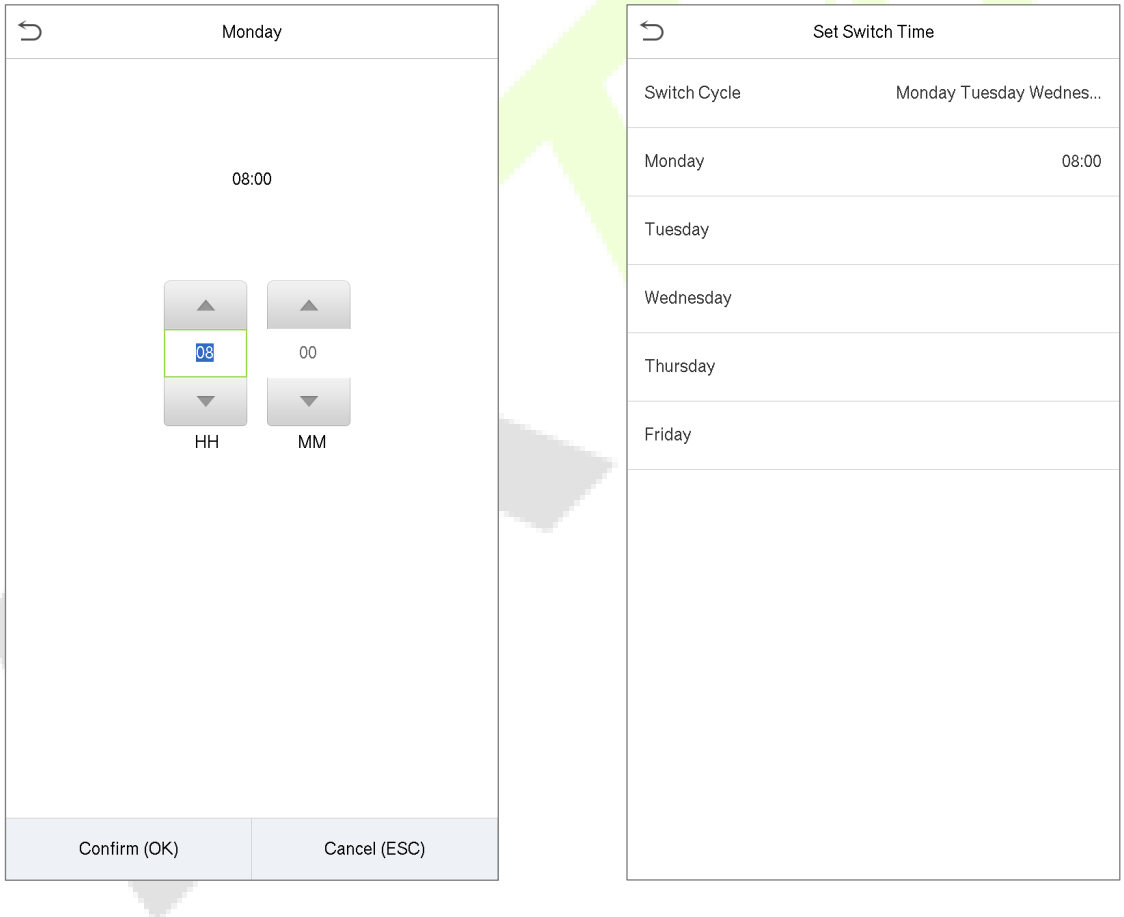
- Si la tecla de acceso directo está configurada como una tecla de estado de perforación (como registro de entrada, salida, etc.), entonces es necesario configurar el valor del estado de perforación (valor válido 0 ~ 250), el nombre y la hora de cambio.

Establecer la hora del cambio

- El tiempo de conmutación se establece de acuerdo con las opciones de estado de perforación. Cuando el **punch statemode** se
- establece en **Modo automático,** debe establecerse el tiempo de conmutación. Sobre el **Tecla de acceso directo** interfaz,
- toque **Establecer SwitchTime** para configurar la hora del cambio.
- Sobre el **Ciclo de cambio** interfaz, seleccione el ciclo de cambio (lunes, martes, etc.) como se muestra en la imagen siguiente.



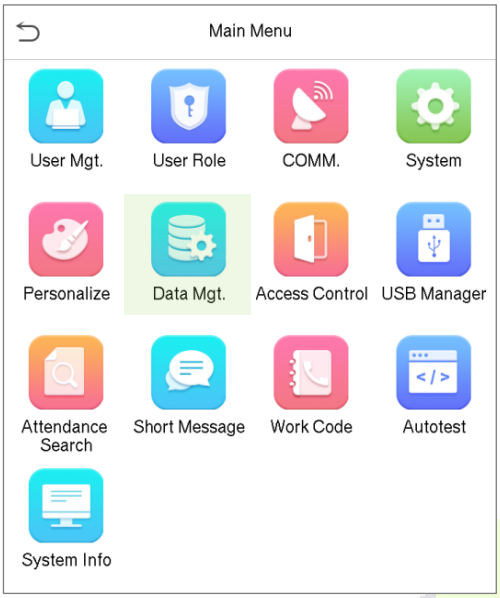
- Una vez que se selecciona el ciclo de cambio, configure el tiempo de cambio para cada día y toque **Okay** para confirmar, como se muestra en la imagen de abajo.

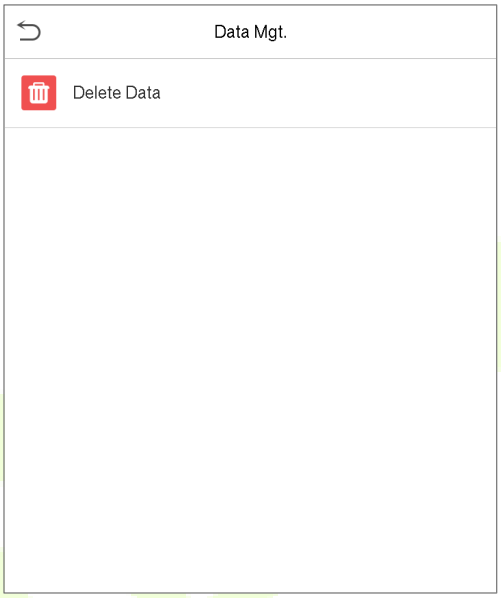


Nota: Cuando la función está configurada como Indefinida, el dispositivo no habilitará la tecla de estado de perforación.

10 Gestión de datos

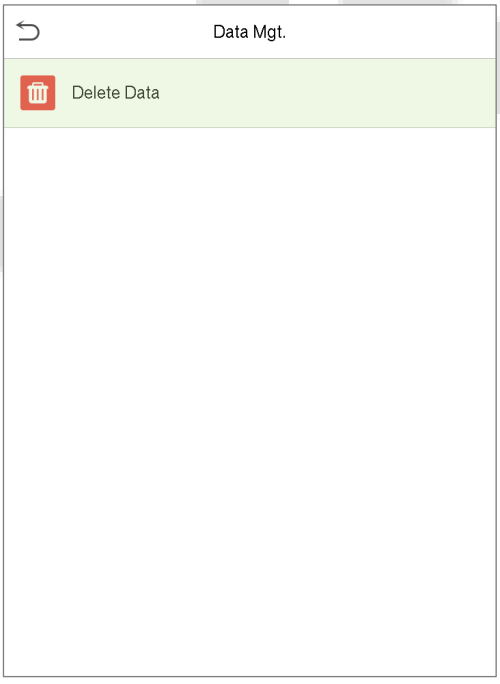
- Sobre el **Menú principal,** grifo **DataMgt.** para eliminar los datos relevantes en el dispositivo.

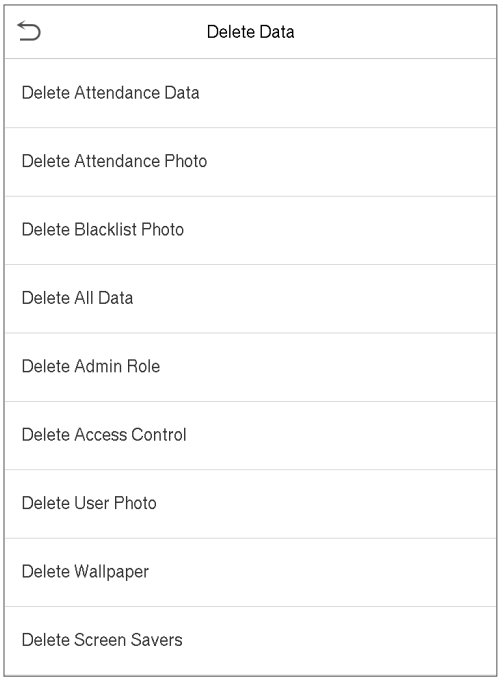




10.1 Borrar datos

- Sobre el **Menú principal,** grifo **Borrar datos** para borrar los datos requeridos.



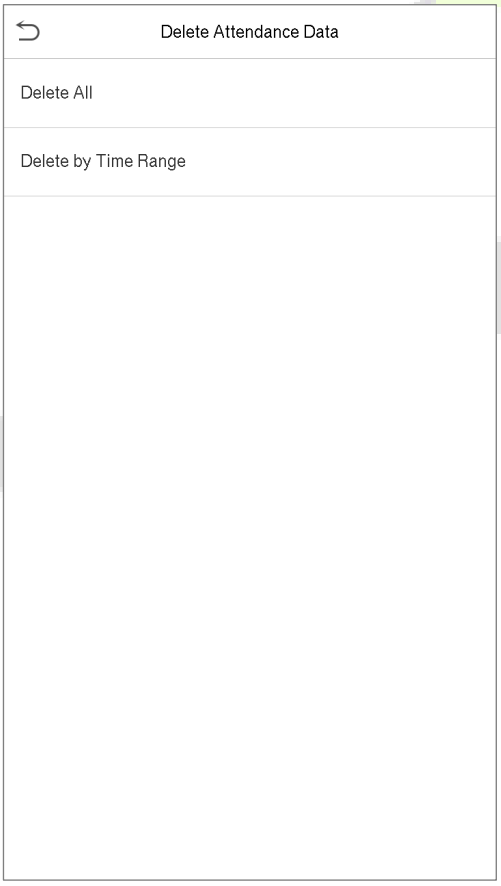


Función descriptiva

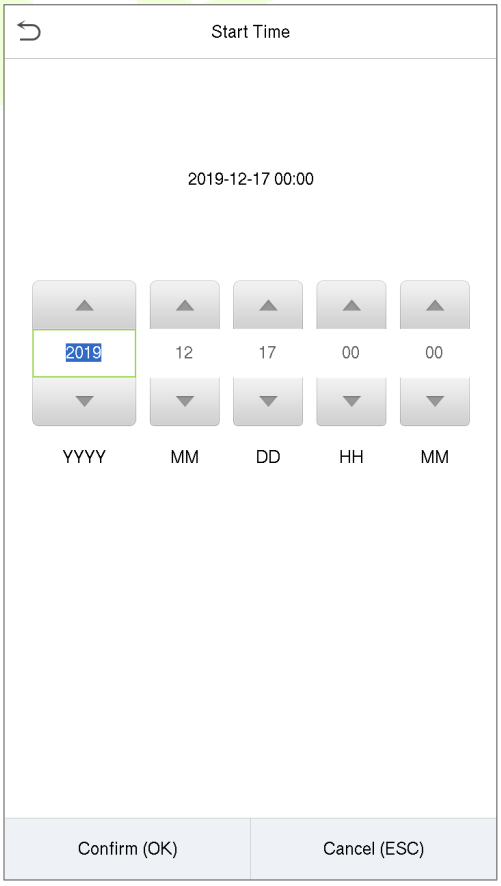
Nombre de la función	Descripción
Eliminar datos de asistencia / registros de acceso	Elimina los datos de asistencia / registros de acceso de forma condicional.

Eliminar foto de asistencia	Elimina las fotos de asistencia del personal designado. Elimina las fotos
Eliminar foto de la lista negra	de las verificaciones fallidas.
Eliminar todos los datos	Elimina los registros de datos y asistencia / registros de acceso de todos los usuarios registrados. Elimina
Eliminar función de administrador	todos los privilegios de administrador.
Eliminar control de acceso	Elimina todos los datos de acceso.
Eliminar foto de usuario	Elimina todas las fotos de usuario del dispositivo. Elimina todos
Eliminar fondo de pantalla	los fondos de pantalla del dispositivo. Elimina todos los
Eliminar protectores de pantalla	protectores de pantalla del dispositivo.

- El usuario puede seleccionar Eliminar todo o Eliminar por intervalo de tiempo al eliminar los datos de asistencia / registros de acceso, fotos de asistencia o fotos de la lista negra.
- Si se selecciona Eliminar por rango de tiempo, entonces es necesario establecer un rango de tiempo específico para eliminar todos los datos dentro del período específico.



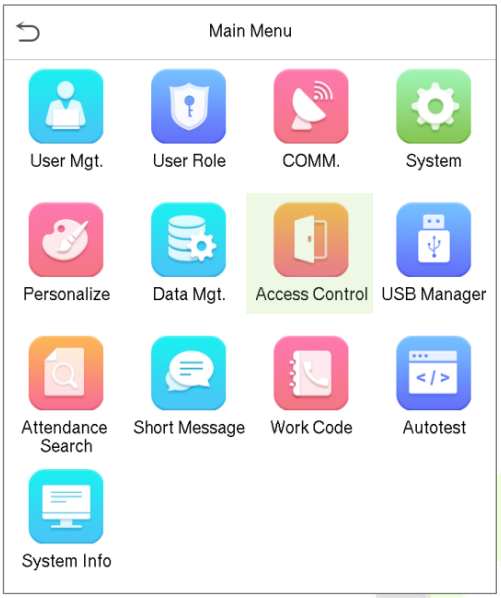
Seleccione Eliminar por rango de tiempo.

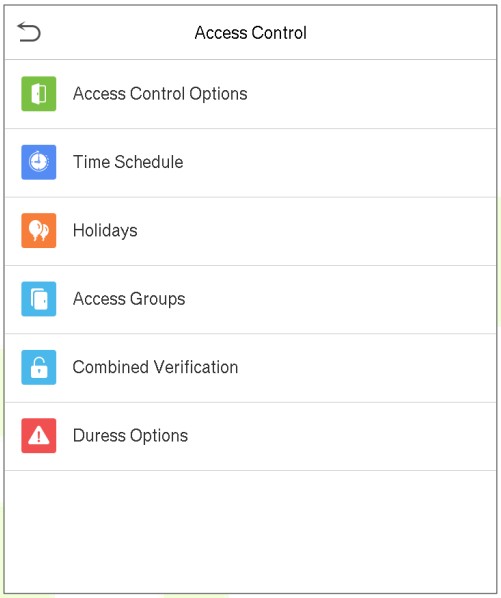


Establezca el intervalo de tiempo y haga clic en Aceptar.

11 Control de acceso

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



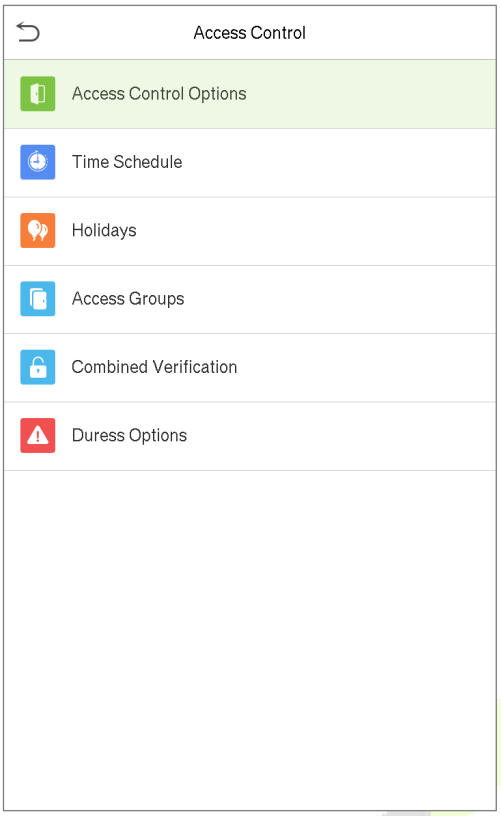


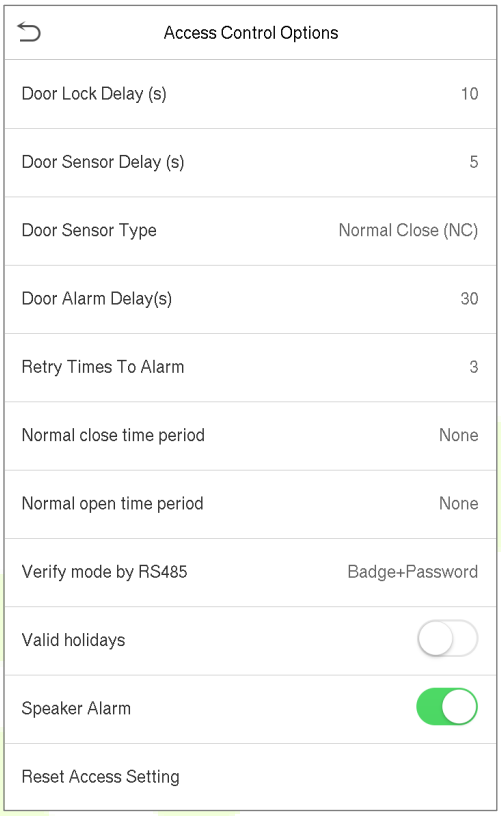
Para acceder, el usuario registrado debe cumplir las siguientes condiciones.

- El tiempo de desbloqueo actual de la puerta correspondiente debe estar dentro de la zona horaria válida del período de tiempo del usuario.
- El grupo de usuarios correspondiente ya debe estar configurado en la combinación de desbloqueo de la puerta (y si hay otros grupos de usuarios, que se configuran en el mismo combo de acceso, también se requiere la verificación de los miembros de ese grupo para desbloquear la puerta).
- En la configuración predeterminada, los nuevos usuarios se asignan al primer grupo con la zona horaria predeterminada del grupo, donde el combo de acceso es "1" y está configurado en estado de desbloqueo de manera predeterminada.

11,1 Opciones de control de acceso

- Sobre el **Control de acceso** interfaz, toque **Opciones de control de acceso** para configurar los parámetros del bloqueo de control para el dispositivo y otros componentes relacionados.





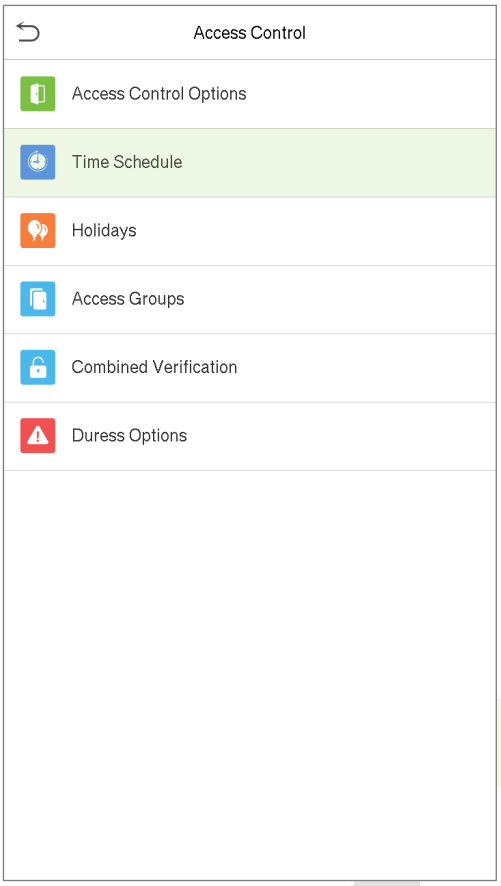
Función descriptiva

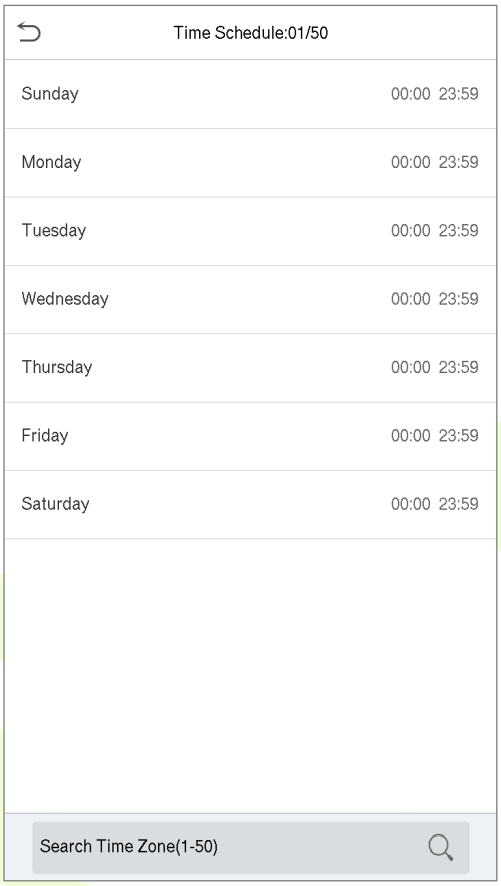
Nombre de la función	Descripción
Retraso de bloqueo de puerta (s)	El tiempo que el dispositivo controla que la cerradura eléctrica esté en estado de desbloqueo. Valor válido: 1 ~ 10 segundos; 0 segundos representa la desactivación de la función.
Retraso (s) del sensor de puerta	Si la puerta no está bloqueada y se deja abierta durante una cierta duración (retardo del sensor de puerta), se activará una alarma. El valor válido del retardo del sensor de puerta varía de 1 a 255 segundos.
Tipo de sensor de puerta	Hay tres tipos de sensores: Ninguno, Apertura normal y Cierre normal. **Ninguna:** Significa que el sensor de puerta no está en uso. **Abierto normal:** Significa que la puerta siempre se deja abierta cuando la energía eléctrica está encendida. **Cierre normal:** Significa que la puerta siempre se deja cerrada cuando la energía eléctrica está encendida.
Retardo (s) de alarma de puerta	Cuando el estado del sensor de la puerta no coincide con el del tipo de sensor de la puerta, se activará una alarma después de un período de tiempo específico, es decir, el Retardo de alarma de puerta. El valor válido varía de 1 a 999 segundos y 0 significa alarma inmediata.
Tiempos de reintento para alarma	Cuando el número de verificaciones fallidas alcanza un valor establecido, que varía de 1 a 9 veces, se disparará una alarma. Si el valor establecido es "Ninguno", la alarma nunca se activará por las verificaciones fallidas.

Nombre de la función	Descripción
Período de tiempo de cierre normal	Período de tiempo programado para el modo de “cierre normal”, de modo que nadie pueda aprovechar el acceso durante este período.
Período de tiempo abierto normal	Período de tiempo programado para el modo de “apertura normal”, de modo que la puerta siempre se deje abierta durante este período.
Verificar modo por RS485	El modo de verificación se utiliza cuando el dispositivo se utiliza como host o esclavo. El modo de verificación admitido incluye Tarjeta / Huella digital, Solo huella digital, Solo tarjeta, Huella digital + Contraseña, Tarjeta + Contraseña, Tarjeta + Huella digital y Tarjeta + Huella digital + Contraseña.
Vacaciones válidas	Configura los ajustes de Período de cierre normal o Período de apertura normal para que sean efectivos en el período de tiempo de vacaciones establecido. Cambie para habilitar o deshabilitar la función durante las vacaciones.
Alarma de altavoz	Transmite una alarma sonora o una alarma de desmontaje desde el local. Cuando la puerta esté cerrada o la verificación sea exitosa, el sistema cancelará la alarma del local.
Restablecer configuración de acceso	Los parámetros de reinicio del control de acceso incluyen retardo de bloqueo de puerta, retardo de sensor de puerta, tipo de sensor de puerta, período de tiempo de cierre normal, período de tiempo de apertura normal, configuración de entrada auxiliar y alarma. Excepto por los datos de control de acceso borrados en Data Mgt. está excluido.

11,2 Horario

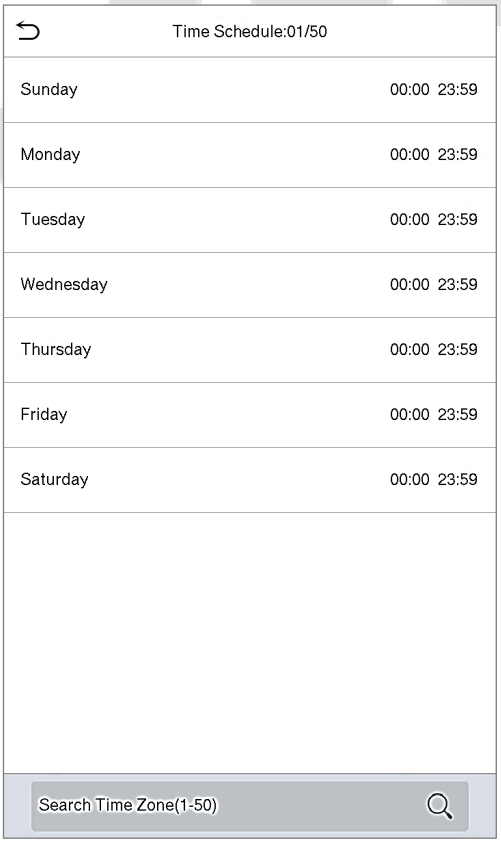
- Sobre el **Control de acceso** interfaz, toque **Horario** para configurar los ajustes de hora. Todo el sistema se puede
- definir hasta **50** Períodos de tiempo.
- Cada período de tiempo representa **7** Zonas horarias, es decir **1** semana, y cada zona horaria es un período estándar de 24 horas por día y el usuario solo puede verificar dentro del período de tiempo válido.
- El formato de zona horaria de cada período de tiempo: HH MM-HH MM, que tiene una precisión de minutos según el reloj de 24 horas.
- Toque el cuadro gris para buscar la zona horaria requerida y especifique el número de zona horaria requerido (puede especificar hasta 50 zonas).





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

- Especifique la hora de inicio y finalización y luego toque **OKAY.**



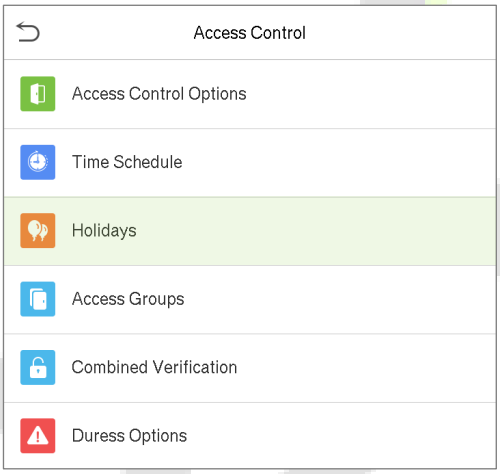
Notas:

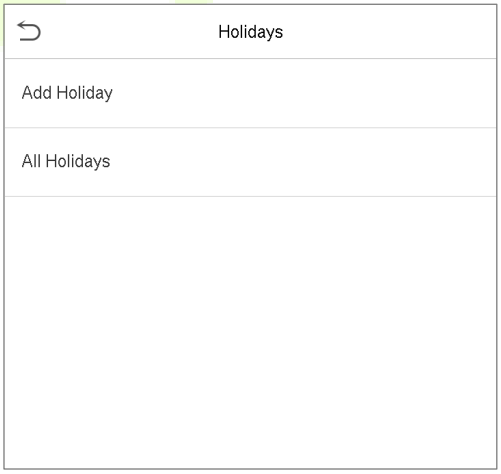
- Cuando la hora de finalización es anterior a la hora de inicio (por ejemplo, 23: 57 ~ 23: 56), indica que el acceso está prohibido durante todo el día.
- Cuando la hora de finalización es posterior a la hora de inicio (por ejemplo, 00: 00 ~ 23: 59), indica que el intervalo es válido.
- El período de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

11,3 Configuración de vacaciones

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

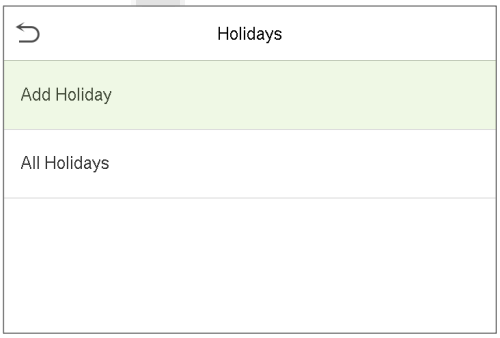
- Sobre el **Control de acceso** interfaz, toque **Días festivos** para configurar el acceso de vacaciones.





Agregar un nuevo feriado

- Sobre el **Días festivos** interfaz, toque **Agregar feriado** para configurar los parámetros de vacaciones.



Editar un feriado

- Sobre el **Días festivos** interfaz, toque un elemento de vacaciones para modificarlo. Grifo **Editar** para modificar los parámetros de vacaciones.

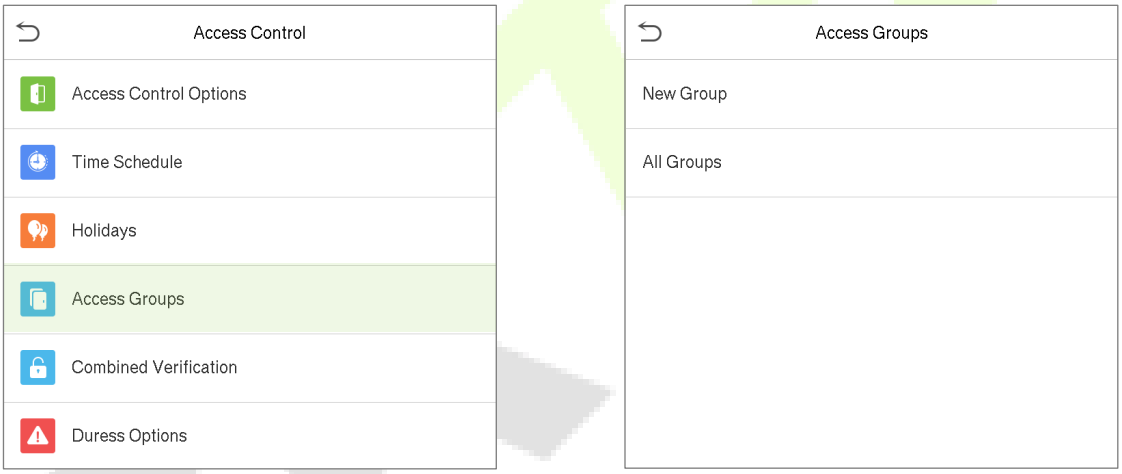
Eliminar un feriado

- Sobre el **Días festivos** interfaz, toque en un elemento de vacaciones para eliminar y toque **Eliminar.** Grifo **Okay** para confirmar la eliminación.

  Después de la eliminación, este día festivo ya no se mostrará en **Todos los días festivos** interfaz.

11,4 Grupos de acceso

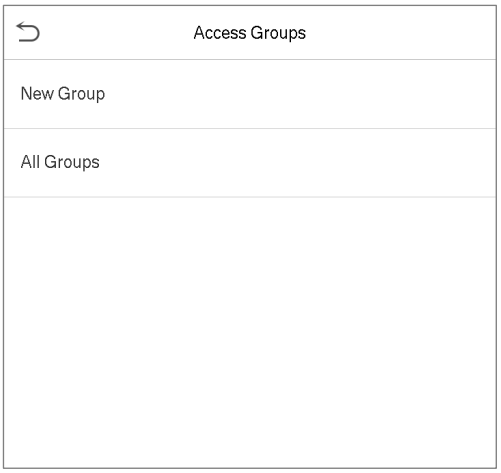
- Sobre el **Control de acceso** interfaz, toque **Grupos de acceso** para administrar fácilmente los diferentes grupos de usuarios en diferentes grupos de acceso.

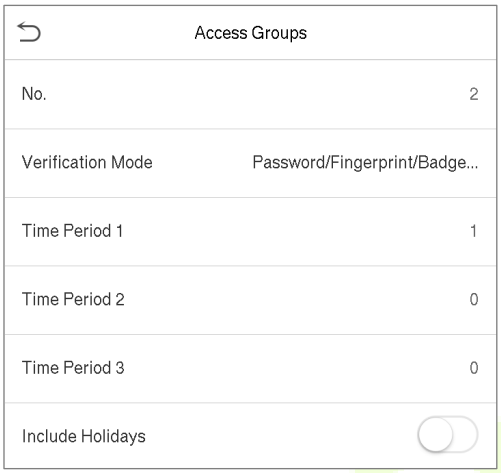


- La configuración del grupo de acceso, como las zonas horarias de acceso, es aplicable a todos los usuarios del grupo de forma predeterminada, donde los usuarios pueden configurar manualmente las zonas horarias según sea necesario.
- Si el modo de autenticación de grupo se superpone con la autenticación individual, la autenticación de usuario tiene prioridad sobre la autenticación de grupo.
- Cada grupo puede establecer un máximo de tres zonas horarias. De forma predeterminada, los usuarios recién inscritos se asignan al Grupo de acceso 1; se pueden asignar a otros grupos de acceso más adelante según el requisito.

Agregar un grupo nuevo

- Sobre el **Grupos de acceso** interfaz, toque **Nuevo grupo** para configurar los parámetros del grupo de acceso.





Nota:

- Hay un grupo de acceso predeterminado numerado 1, que no se puede borrar, pero se puede modificar. El número de grupo de
- acceso no se puede modificar después de configurarlo.
- Cuando se establece que las vacaciones sean válidas, el personal de un grupo solo podrá abrir la puerta cuando la zona horaria del grupo se superponga con el período de vacaciones.
- Cuando se establece que las vacaciones no son válidas, el tiempo de control de acceso del personal de un grupo no se ve afectado durante las vacaciones.

Editar un grupo

- En **Todos los grupos** interfaz, seleccione el elemento del grupo de acceso que desee modificar.
- Grifo **Editar** y modificar los parámetros del grupo de acceso.

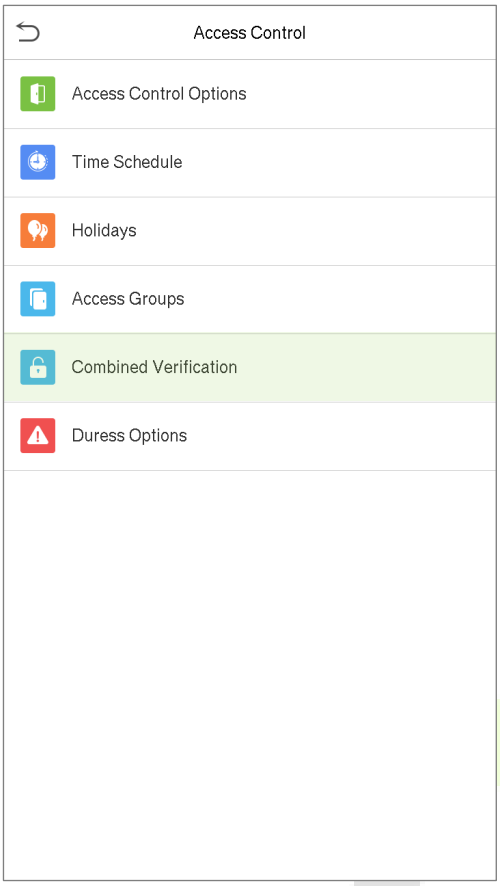
Eliminar un grupo

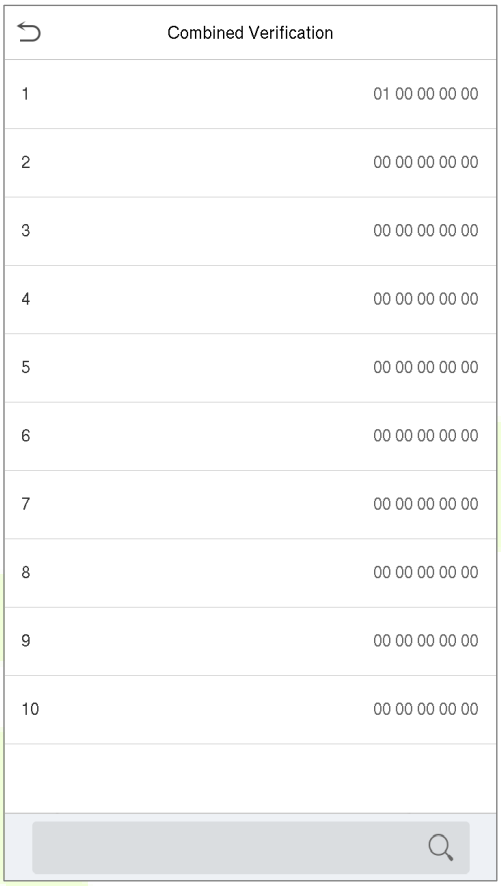
- En **Todos los grupos** interfaz, seleccione el elemento del grupo de acceso que desee eliminar y haga clic en **Eliminar.**
- Grifo **Okay** para confirmar la eliminación. El grupo de acceso eliminado ya no se mostrará en la interfaz de Todos los grupos.

11,5 Configuración de verificación combinada

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

- Sobre el **Control de acceso** interfaz, toque **Verificación combinada** para configurar los ajustes de verificación combinados.





- En la interfaz de verificación combinada, toque la combinación de desbloqueo de puerta que desee configurar y toque el **arriba** y **abajo** flechas para ingresar el número de combinación y luego toque **Okay**

Por ejemplo:

- los **Combinación de desbloqueo de puerta 1** se establece como (**01 03 05 06 08),** indicando que el desbloqueo

  La combinación 1 consta de 5 personas, y las 5 personas son de 5 grupos, es decir, **Grupo de control de acceso** 1 (Grupo CA 1), Grupo CA 3, Grupo CA 5, Grupo CA 6 y Grupo CA 8, respectivamente.

- los **Combinación de desbloqueo de puerta 2** se establece como (**02 02 04 04 07),** indicando que el desbloqueo

  la combinación 2 consta de 5 personas; los dos primeros son del grupo 2 de CA, los dos siguientes son del grupo 4 de CA y la última persona es del grupo 7 de CA.

- los **Combinación de desbloqueo de puerta 3** se establece como (**09 09 09 09 09),** indicando que hay 5 personas en esta combinación; y todos ellos son del grupo AC 9.

- los **Combinación de desbloqueo de puerta 4** se establece como (**03 05 08 00 00),** indicando que el desbloqueo

  La combinación 4 consta de solo 3 personas. La primera persona es del grupo AC 3, la segunda persona es del grupo AC 5 y la tercera persona es del grupo AC 8.

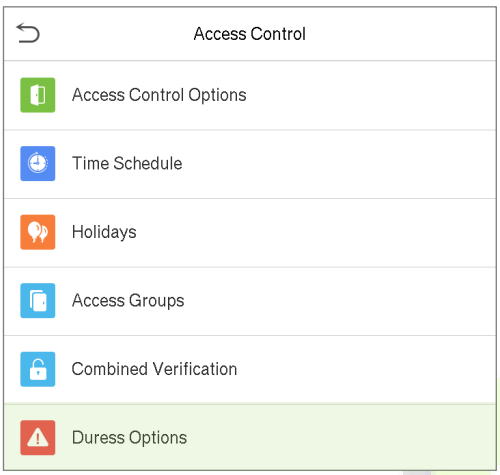
Eliminar una combinación de desbloqueo de puertas

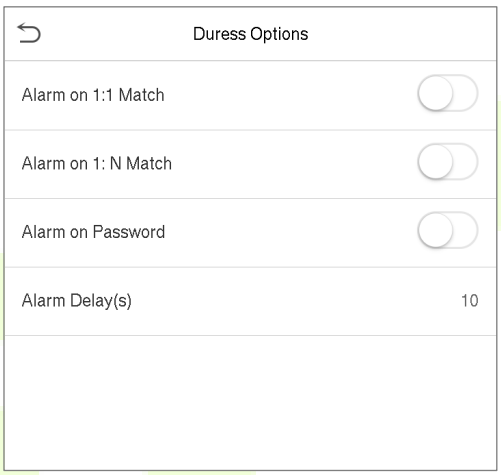
- Establezca todas las combinaciones de desbloqueo de puertas en 0 si desea eliminar todas las combinaciones de desbloqueo de puertas.

11,6 Configuración de opciones de coacción

Una vez que un usuario activa la función de verificación de coacción con un método o métodos de autenticación específicos, y cuando se encuentra bajo coerción y se autentica mediante la verificación de coacción, el dispositivo desbloqueará la puerta como de costumbre, pero al mismo tiempo, se emitirá una señal. enviado para activar la alarma.

- Sobre el **Control de acceso** interfaz, toque **Opciones de coacción** para configurar los ajustes de coacción.



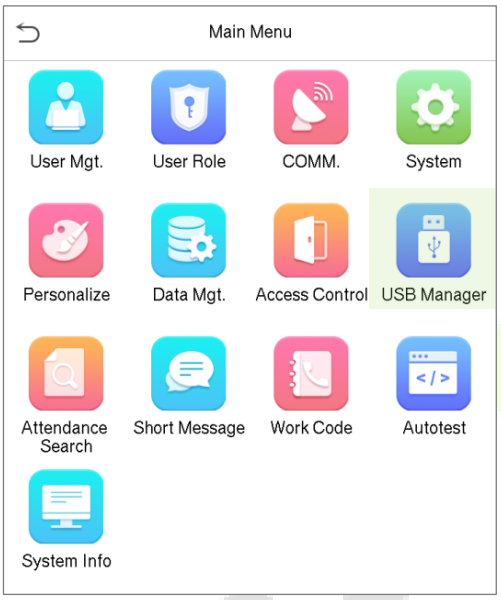


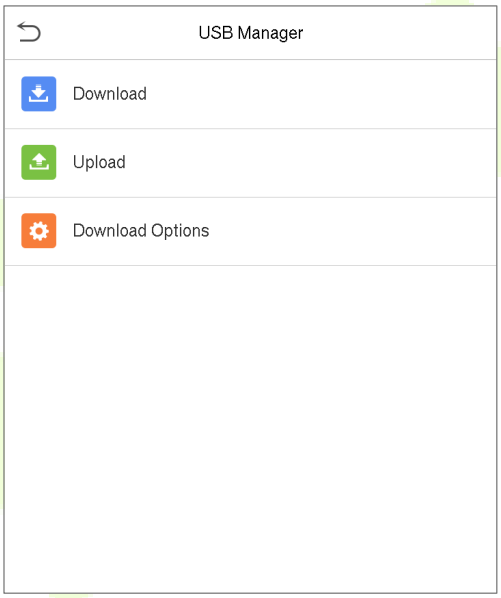
Función descriptiva

Nombre de la función	Descripción
Alarmon 1: 1 Verificación	Cuando un usuario usa cualquier huella digital para realizar la verificación 1: 1, se generará una señal de alarma solo cuando la verificación 1: 1 sea exitosa; de lo contrario, no habrá señal de alarma.
Alarmon 1: N Identificación	Cuando un usuario usa cualquier huella dactilar para realizar la verificación 1: N, se generará una señal de alarma solo cuando la identificación 1: N sea exitosa; de lo contrario, no habrá señal de alarma.
Alarmon Password	Cuando un usuario usa el método de verificación de contraseña, se generará una señal de alarma solo cuando la verificación de contraseña sea exitosa; de lo contrario, no habrá señal de alarma.
Retraso de alarma (s)	La señal de alarma no se transmitirá hasta que transcurra el tiempo de retardo de la alarma. El valor varía de 1 a 999 segundos.

12 USBManager

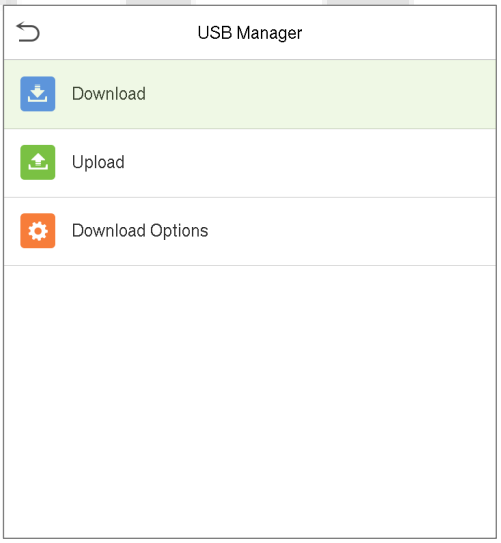
- Sobre el **Menú principal,** grifo **USBManager** para administrar los datos a través de una unidad USB.
- Puede importar información de usuario, acceder a datos y otros datos desde una unidad USB a la computadora u otros dispositivos.
- Antes de cargar o descargar datos desde o hacia la unidad USB, primero inserte la unidad USB en la ranura USB.

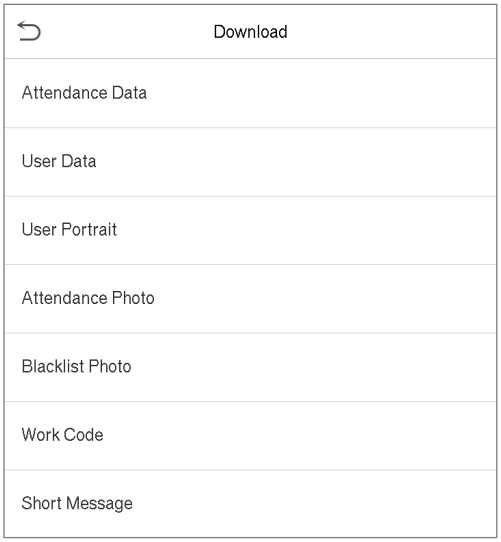




12,1 Descargar

- Sobre el **Administrador USB** interfaz, toque **Descargar** para descargar los datos necesarios del dispositivo a la unidad USB.



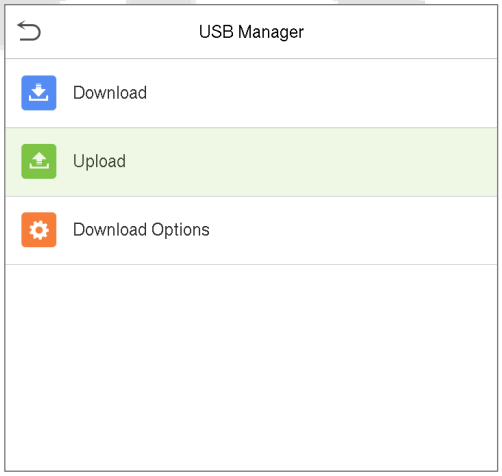


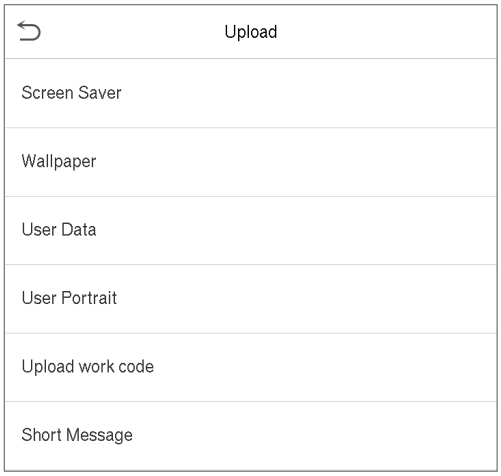
Función descriptiva

Nombre de la función	Descripciones
Datos de asistencia	Permite descargar los datos de asistencia almacenados en el dispositivo dentro de un período de tiempo específico o todos los datos de asistencia del dispositivo a la unidad USB.
Datos del usuario	Permite descargar toda la información del usuario desde el dispositivo a la unidad USB.
Retrato de usuario	Permite descargar todas las imágenes de usuario desde el dispositivo a la unidad USB.
Asistencia Foto	Permite descargar las fotos de asistencia almacenadas en el dispositivo dentro de un período de tiempo especificado o todas las fotos de asistencia del dispositivo a la unidad USB. El formato de imagen es JPG
Foto de la lista negra	Permite descargar fotos de la lista negra tomadas después de verificaciones fallidas dentro de un período de tiempo especificado o todas las fotos tomadas después de verificaciones fallidas desde el dispositivo a la unidad USB.
Código de trabajo	Permite descargar todos los códigos de trabajo del dispositivo a la unidad USB.
Mensaje corto	Permite descargar un conjunto de mensajes cortos públicos o privados, que son leídos por objetos especificados dentro del tiempo especificado después de la asistencia, facilitando la transmisión de información.

12,2 Subir

- Sobre el **Administrador USB** interfaz, toque **subir** para cargar los datos necesarios en el dispositivo desde la unidad USB.



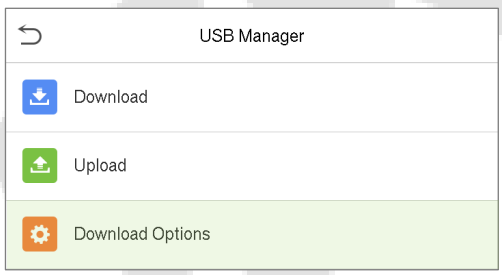


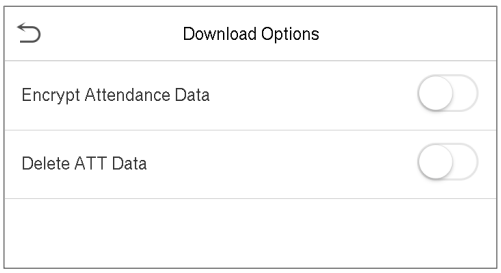
Función descriptiva

Nombre de la función	Descripción
Salvapantallas	Puede cargar el protector de pantalla desde la unidad USB al dispositivo. Antes de cargar, puede seleccionar **Cargar imagen seleccionada** o **Subir todo imágenes.**
Fondo de pantalla	Puede cargar fondos de pantalla desde la unidad USB al dispositivo. Antes de cargar, puede seleccionar **Cargar imagen seleccionada** o **Sube todas las imágenes.** Las imágenes se mostrarán en la pantalla después de la configuración manual.
Datos del usuario	Puede cargar toda la información del usuario desde una unidad USB al dispositivo.
Retrato de usuario	Puede cargar la imagen JPG nombrada con una identificación de usuario desde la unidad USB al dispositivo. Antes de cargar, puede seleccionar **Cargar imagen actual** o **Subir todo Imágenes.**
Subir código de trabajo	Puede cargar códigos de trabajo desde la unidad USB al dispositivo.
Mensaje corto	Puede cargar un conjunto de mensajes cortos públicos o privados, que son leídos por objetos especificados dentro del tiempo especificado después de la asistencia, lo que facilita la transmisión de información.

12,3 Opciones de descarga

- Sobre el **USBManager** interfaz, toque **Opciones de descarga** para configurar el proceso de descarga requerido.



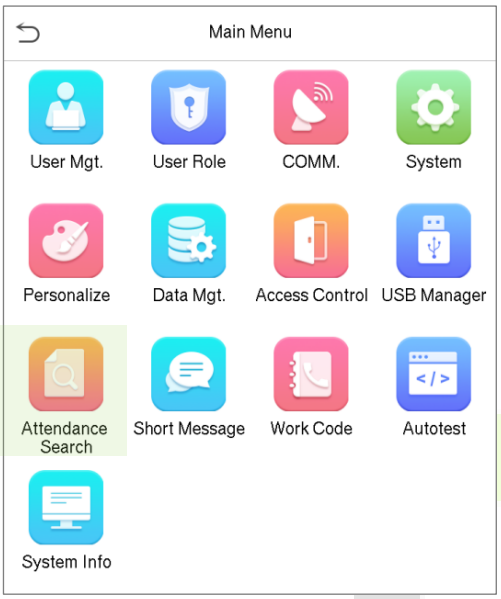


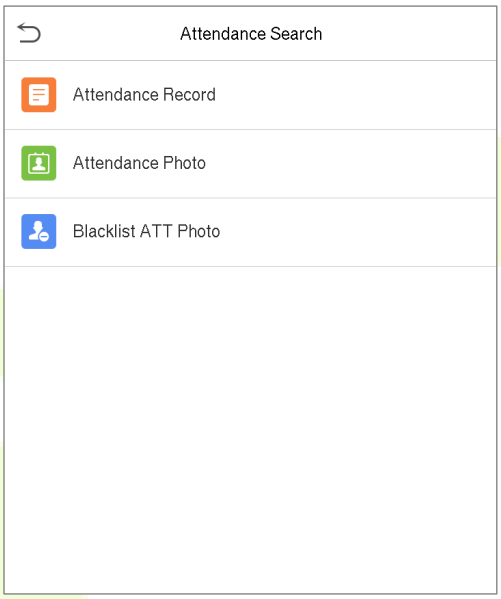
- **Encriptar datos de asistencia:** Palanca **Cifrar datos de asistencia** para habilitar o deshabilitar el cifrado para datos de asistencia.
- **Eliminar datos ATT:** Palanca **Eliminar datos ATT** para habilitar o deshabilitar la eliminación de los datos de asistencia.

Nota: Los datos de asistencia cifrados solo se pueden importar en el software con la versión Access 3.5.

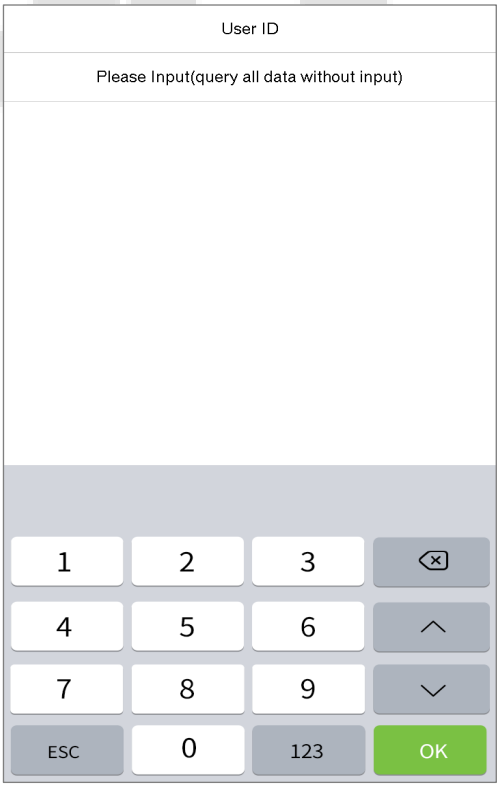
13 Búsqueda de asistencia

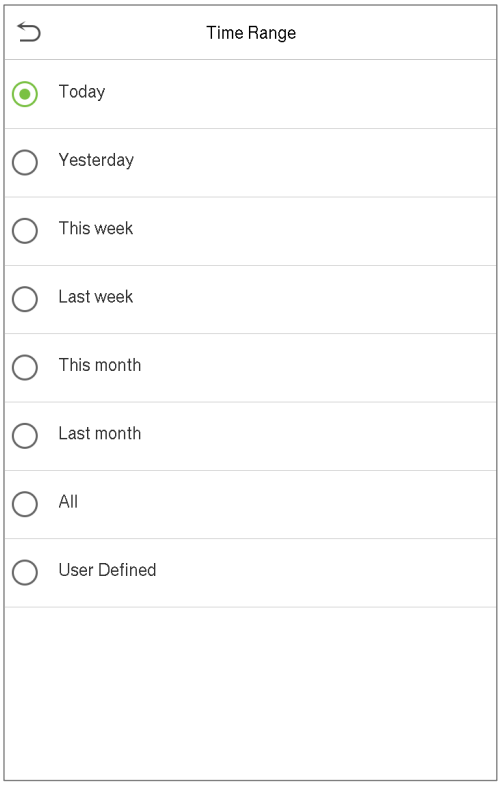
- Una vez que se verifica la identidad de un usuario, el registro de asistencia / acceso se guardará en el dispositivo. Esta función permite a los usuarios verificar sus registros de asistencia / acceso.
- Sobre el **Menú principal,** grifo **Búsqueda de asistencia** para buscar el registro de acceso / asistencia requerido.



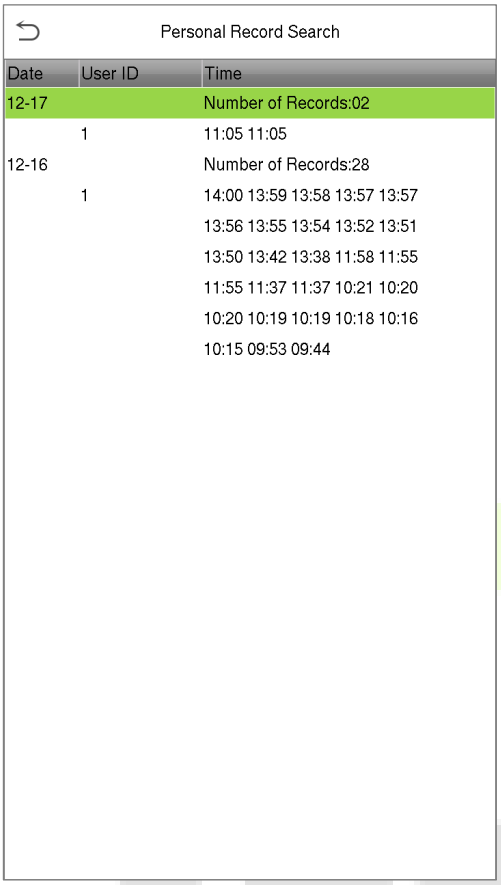


- El proceso de búsqueda de fotos de asistencia y listas negras es similar al de buscar registros de asistencia / acceso. El siguiente es un ejemplo de búsqueda de registros de asistencia / acceso.
- Sobre el **Búsqueda de asistencia** interfaz, toque **Registro de asistencia / acceso** para buscar el requerido grabar.



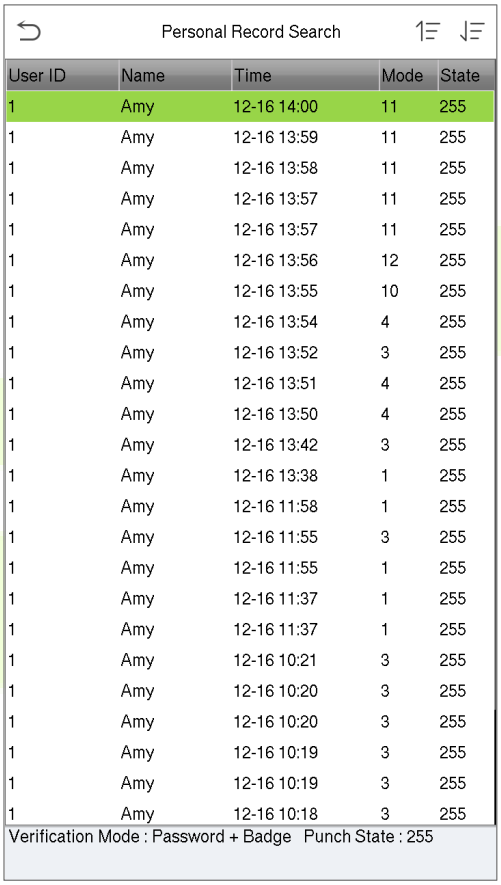


- Ingrese la ID de usuario que desea buscar y toque Aceptar.
- Si desea buscar registros de todos los usuarios, toque Aceptar sin proporcionar ninguna identificación de usuario.



- Una vez que la búsqueda de registros sea exitosa, toque el registro resaltado en verde para ver sus detalles.

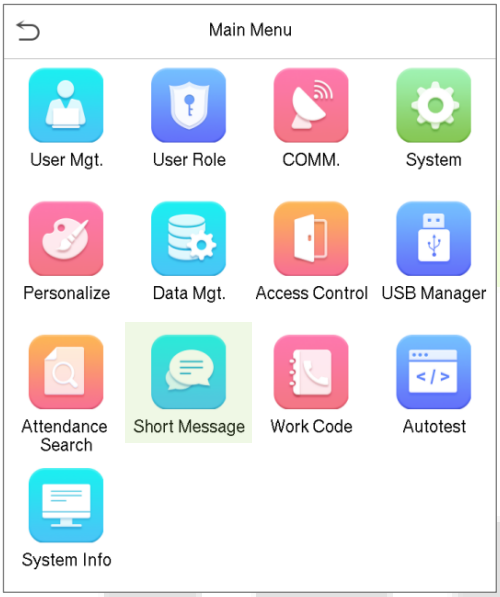
- Seleccione el intervalo de tiempo desde el que se deben buscar los registros.

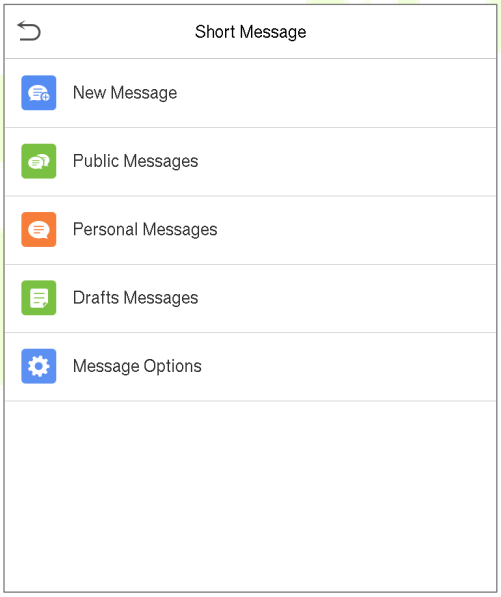


- La figura anterior muestra los detalles del registro seleccionado.

14 Mensaje corto

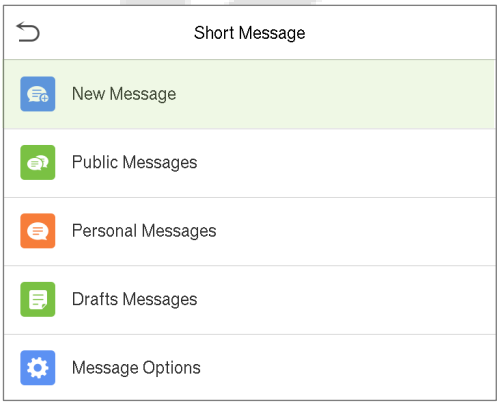
- Sobre el **Menú principal,** grifo **Mensaje corto** para configurar los mensajes cortos.
- SMS es similar al aviso. El operador puede editar el contenido del aviso por adelantado y convertirlo en SMS y mostrarlo en la pantalla.
- SMS incluye SMS comunes y SMS individuales. Si se configura un SMS común, el SMS común icono se mostrará en la columna de información en la parte superior de la interfaz de espera en el tiempo especificado.
- Si se configura un SMS individual, el empleado que puede recibir SMS puede verlo después de una asistencia exitosa.

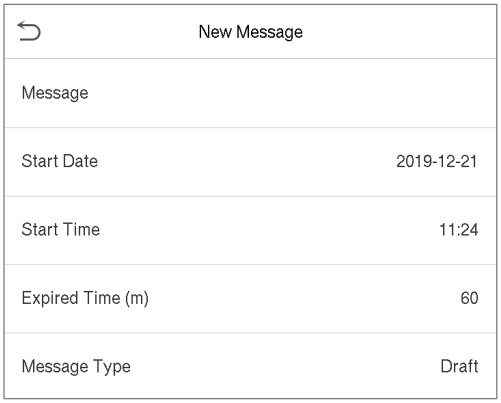




14.1 Agregar un nuevo mensaje corto

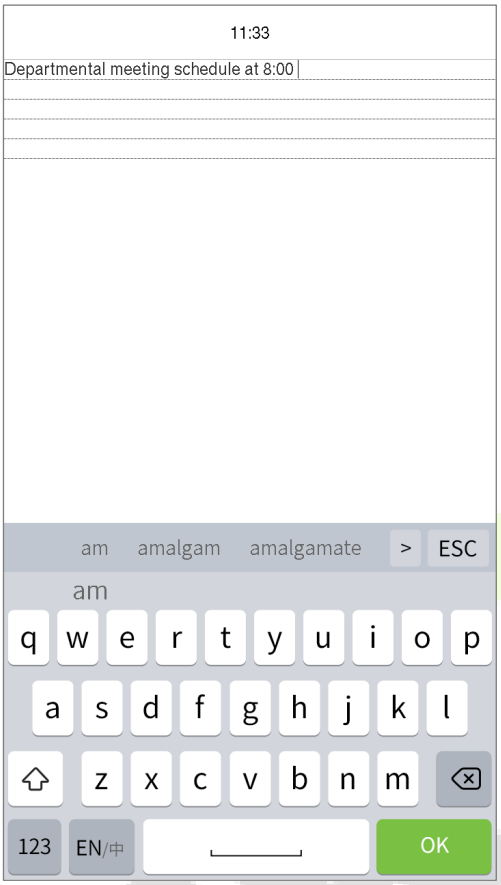
- Sobre el **Mensaje corto** interfaz, toque **Nuevo mensaje** para agregar un nuevo mensaje corto.





Proporcionar el contenido

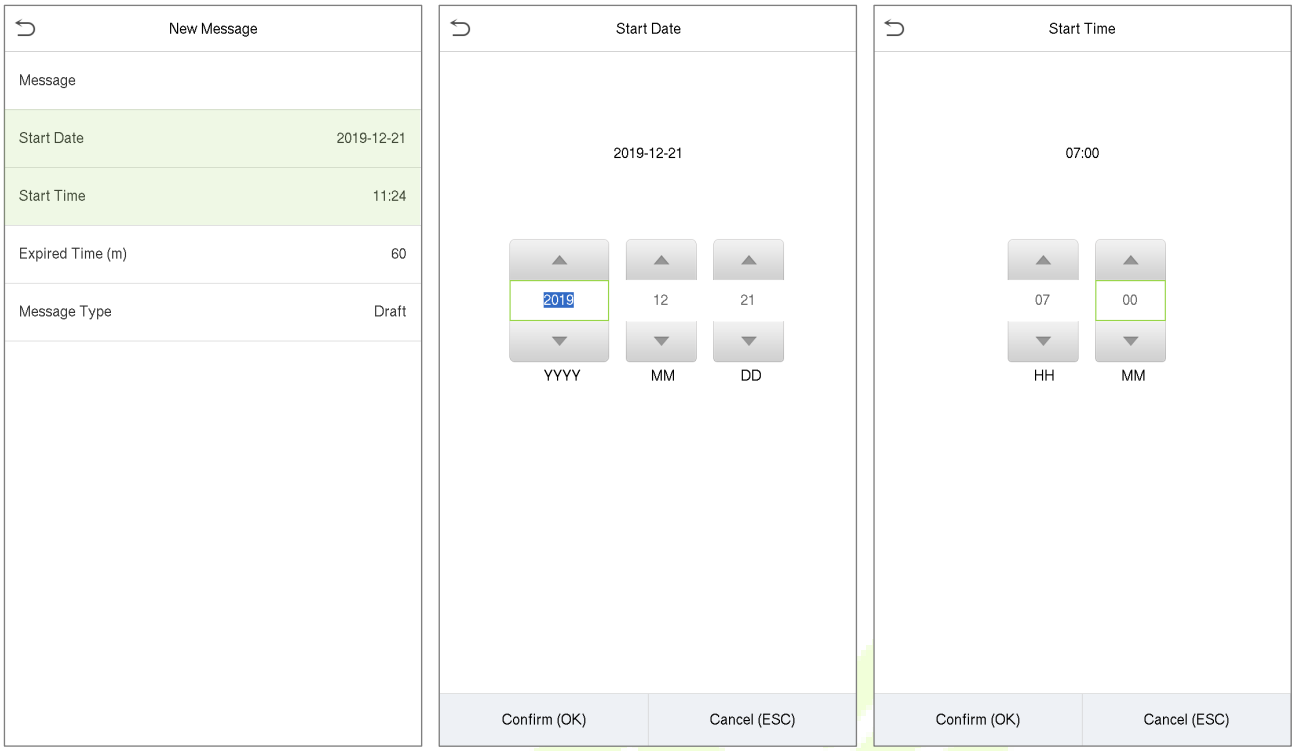
- Sobre el **Mensaje corto** interfaz, proporcione el contenido del mensaje y toque **Confirmar (OK)** para guardar el contenido y salir de la interfaz de mensajes.



Establecer la fecha y hora de inicio

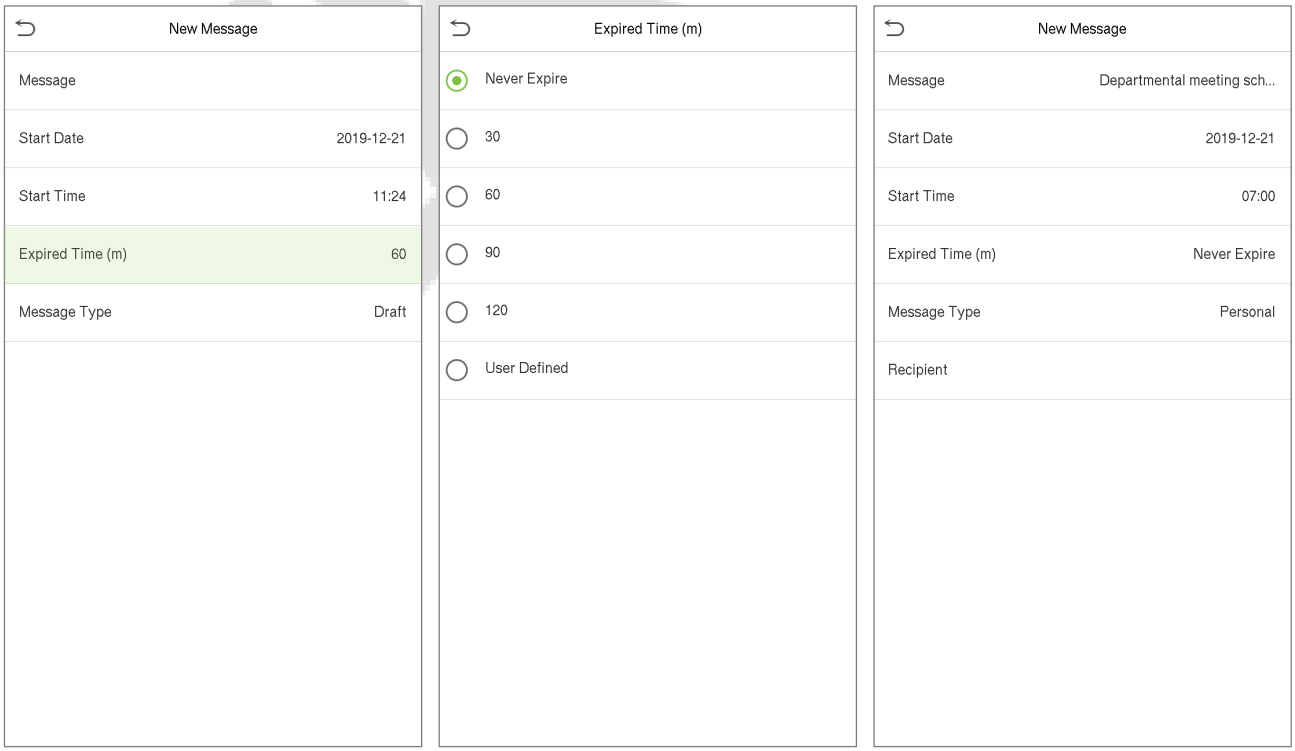
- Sobre el **Nuevo mensaje** interfaz, toque el **Fecha de inicio** y **Hora de inicio** para establecer el período de envío del mensaje corto creado.

- La fecha y la hora se habilitarán una vez que se proporcione el contenido del mensaje corto.



Configuración del tiempo vencido (m)

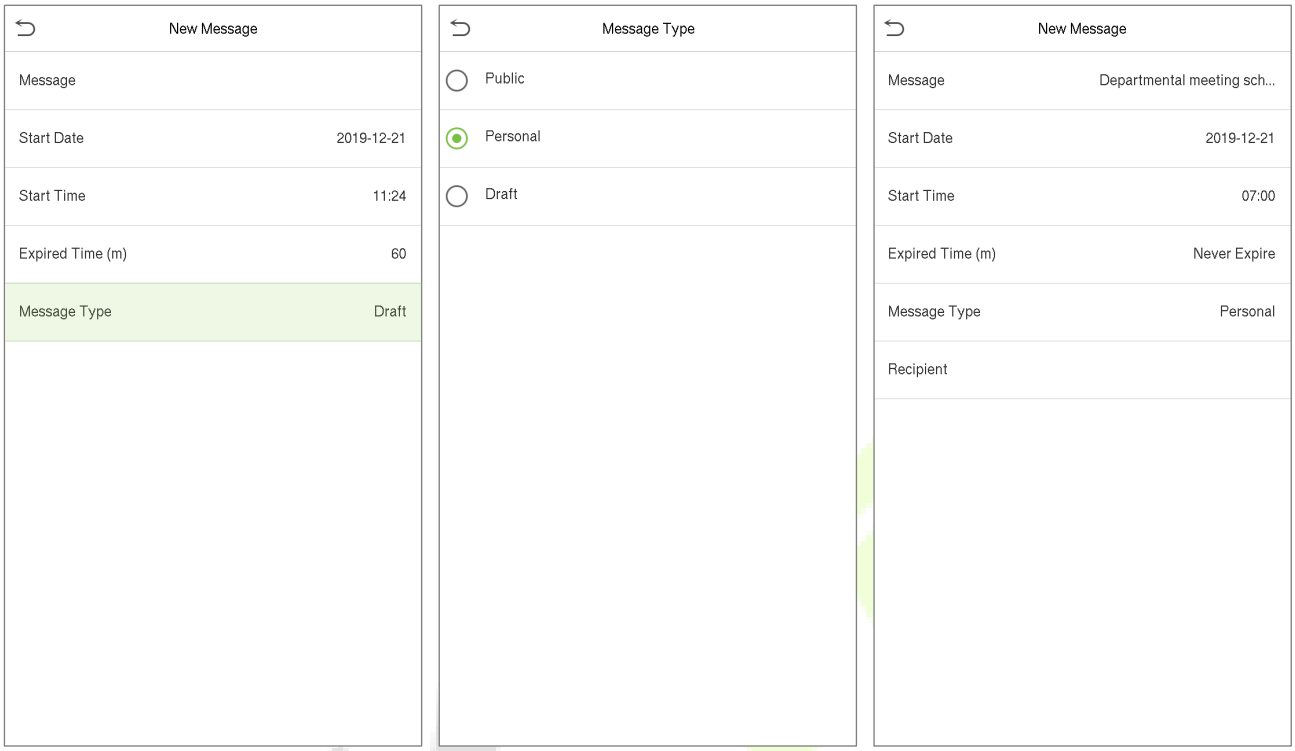
- Sobre el **Nuevo mensaje** interfaz, toque el **Tiempo expirado** para establecer el período de validez del SMS.
- Esto muestra que el SMS aparecerá dentro del tiempo efectivo y el mensaje no se mostrará más allá del tiempo de vencimiento.



Nota: Para los mensajes cortos públicos, el período efectivo también comprende el período de visualización. Para los mensajes cortos privados, debe establecer tanto el período de tiempo efectivo como el período de visualización. Es decir, el período de visualización

de un mensaje corto privado se puede ver cuando ingresa o cierra durante el período de vigencia del mensaje.

Configuración del tipo de mensaje



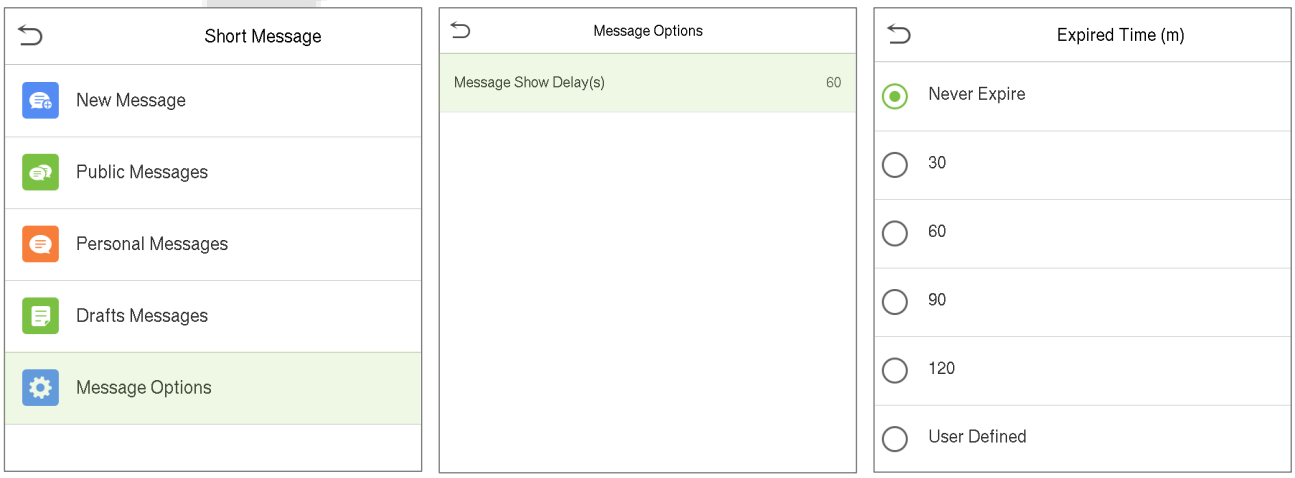
Público: El mensaje será visto por todas las personas.

Personal: Solo las personas seleccionadas verán el mensaje.

Sequía: Almacena el mensaje de texto que escribió hasta ahora, para que pueda agregar más contenido más tarde o enviarlo más tarde.

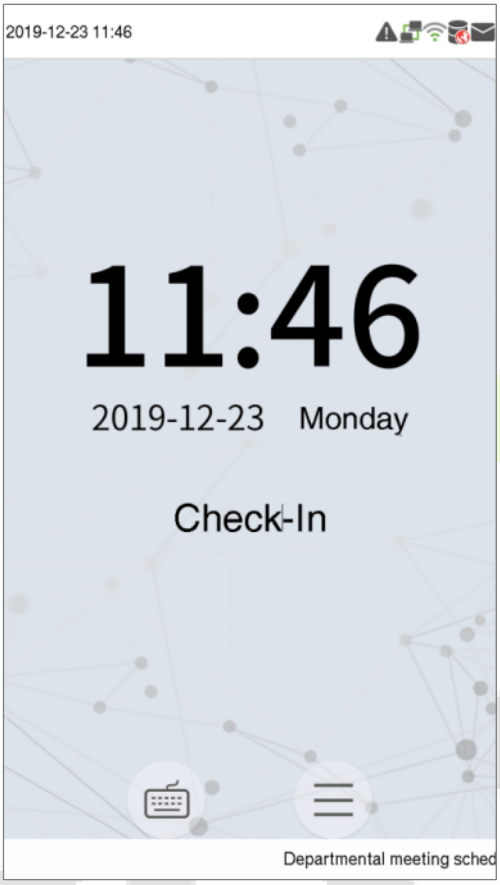
14,2 Opciones de mensaje

- Sobre el **Mensaje corto** interfaz, toque **Opciones de mensaje** para configurar el tiempo de retardo de la visualización de mensajes personales en la interfaz inicial.



14.3 Ver los mensajes públicos y el mensaje personal

- Después de configurar un mensaje corto público, el icono de mensaje corto se muestra en la parte superior derecha de la interfaz principal, y el contenido de mensajes cortos públicos se mostrará en el modo de desplazamiento a continuación.
- El contenido de un mensaje corto personal se muestra después de la autenticación de usuario exitosa.



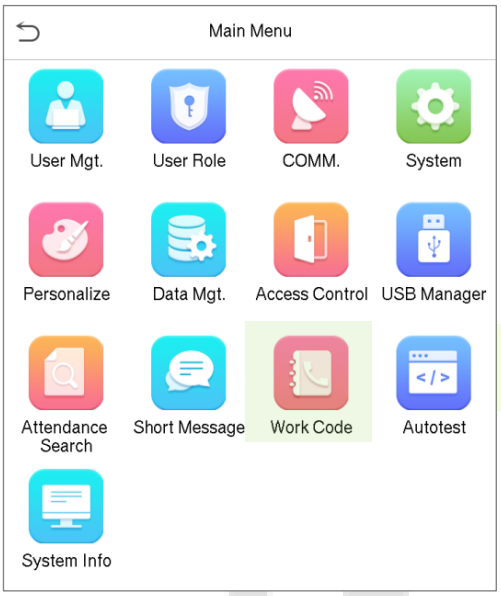
El mensaje corto público se mostrará en la parte inferior de la interfaz.

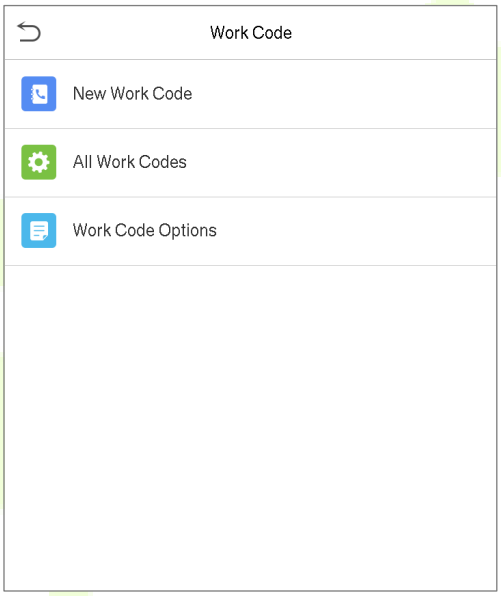
El mensaje corto personal se mostrará después de la autenticación de usuario exitosa.

15 Código de trabajo

Los ingresos de los empleados están sujetos a sus registros de asistencia. Los empleados pueden participar en diferentes tipos de trabajo que pueden variar con los períodos de tiempo. Teniendo en cuenta que los salarios varían con los tipos de trabajo, la terminal FFR proporciona un parámetro para indicar el tipo de trabajo correspondiente para cada registro de asistencia para facilitar la comprensión rápida de los diferentes status quo de asistencia durante el manejo de los datos de asistencia.

- Sobre el **Menú principal,** grifo **Código de trabajo** para configurar los ajustes del código de trabajo.





15,1 Agregar un código de trabajo

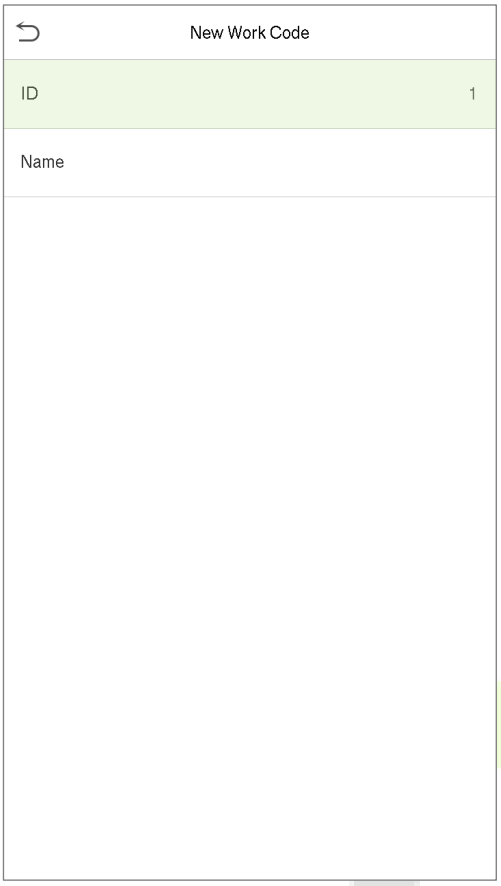
- Sobre el **Código de trabajo** interfaz, toque **Código de obra nueva** para agregar un código de obra nueva.
- Sobre el **Código de obra nueva** interfaz, complete los siguientes detalles.

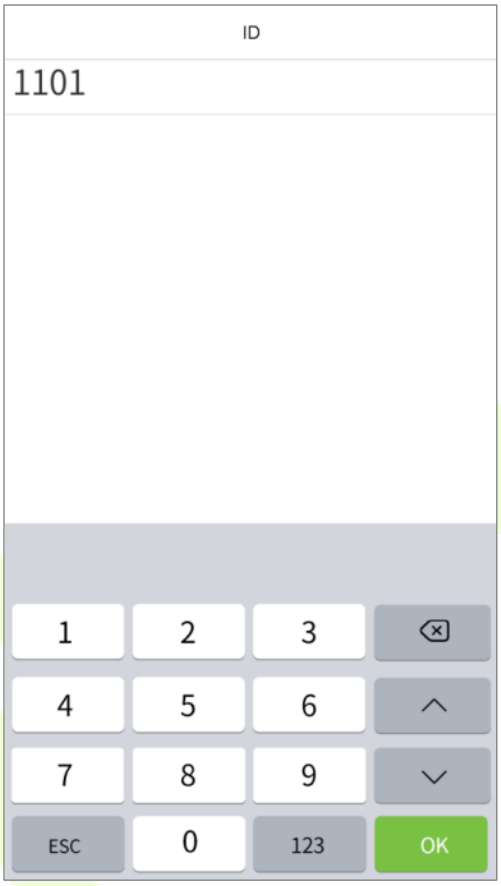
  CARNÉ DE IDENTIDAD: Proporcione el código único del código de trabajo.

  Nombre: Proporcione el nombre del código de trabajo.

Editar una identificación

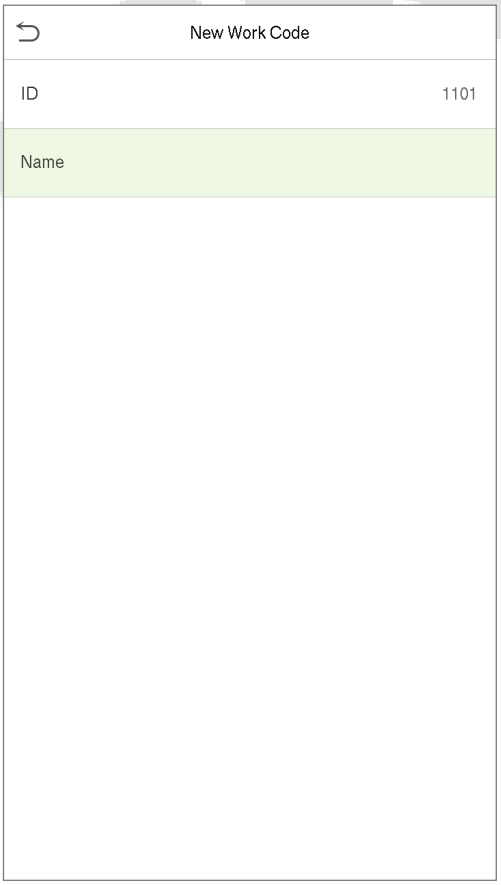
- Sobre el **Código de obra nueva** interfaz, toque el campo ID para editar la ID.

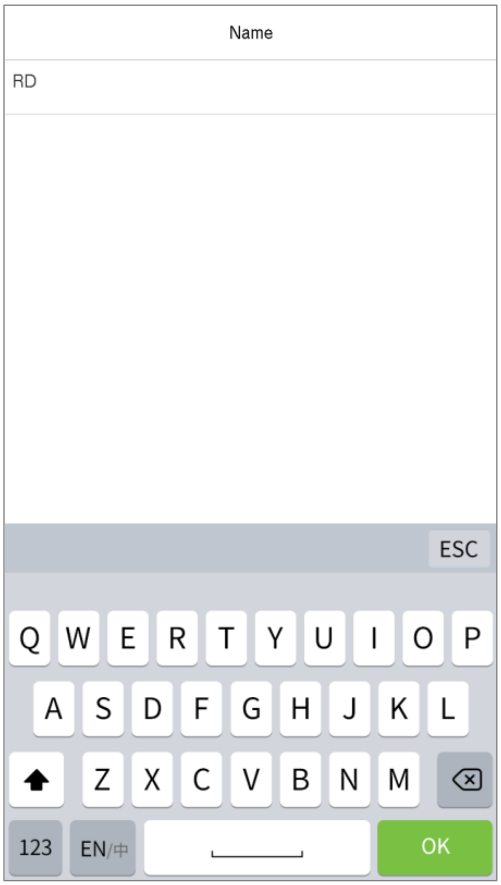




Editando un nombre

- Sobre el **Código de obra nueva** interfaz, toque el campo ID para editar la ID.

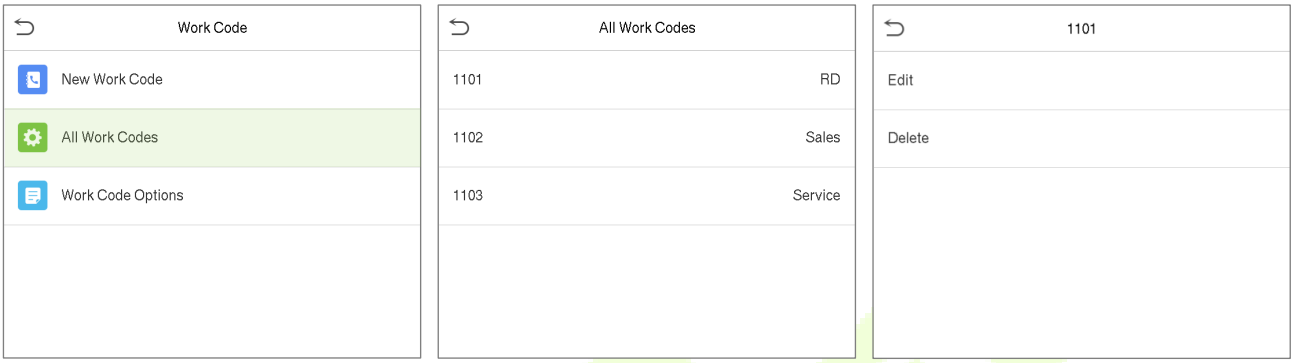




15,2 Lista de todos los códigos de trabajo

Puede ver, editar y eliminar códigos de trabajo en Todos los códigos de trabajo. El proceso de editar un código de trabajo es el mismo que el de agregar un código de trabajo, excepto que no se permite modificar la identificación.

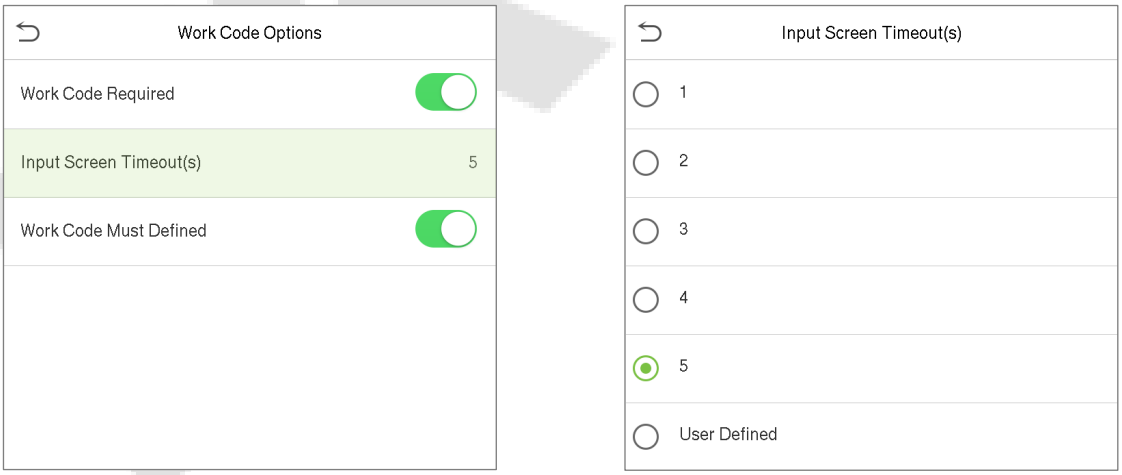
- Sobre el **Código de trabajo** interfaz, toque **Código AllWork** para ver y editar el código de trabajo requerido.



15,3 Opciones de código de trabajo

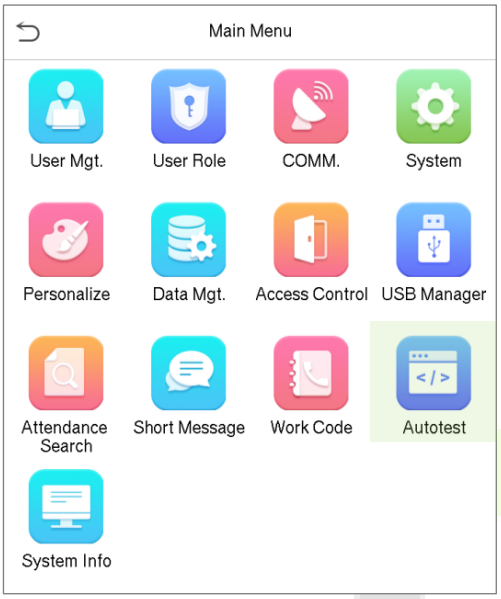
Para establecer si se debe ingresar el código de trabajo y si el código de trabajo ingresado debe existir durante la autenticación.

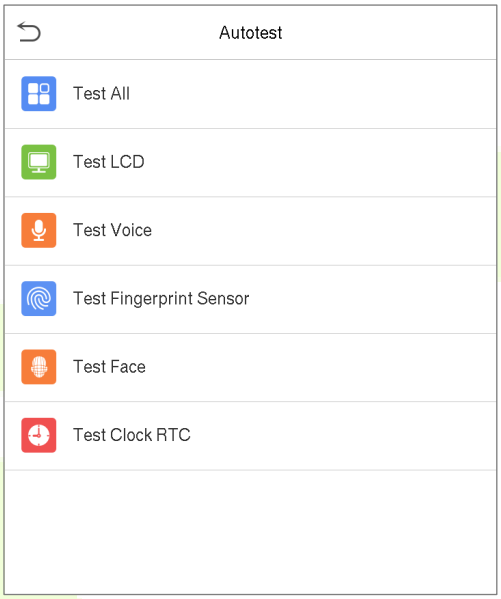
- Sobre el **Código de trabajo** interfaz, toque **Opciones de código de trabajo** para configurar los ajustes del código de trabajo.



dieciséis Auto prueba

- Sobre el **Menú principal,** grifo **Auto prueba** para probar automáticamente si todos los módulos del dispositivo funcionan correctamente, lo que incluye la pantalla LCD, la voz, el sensor de huellas dactilares, la cámara y el reloj en tiempo real (RTC).



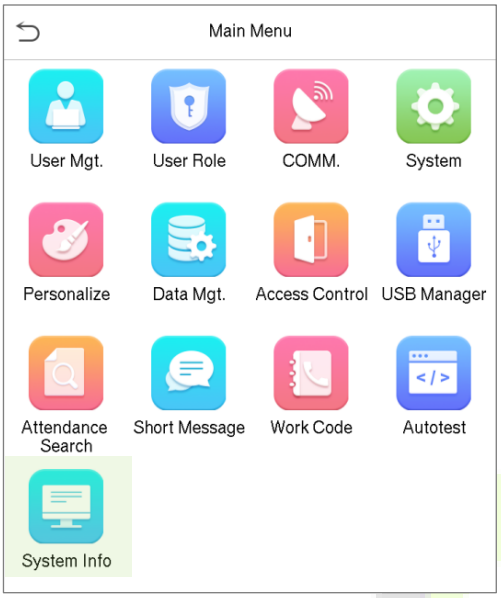


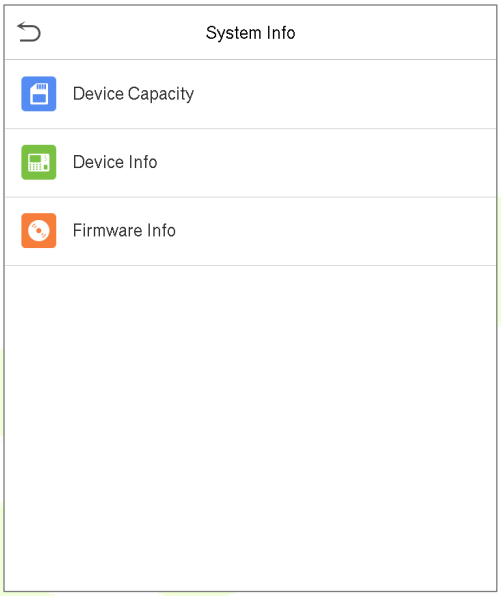
Función descriptiva

Nombre de la función	Descripción
Probar todo	Para probar automáticamente la pantalla LCD, el audio, la cámara y el reloj en tiempo real (RTC).
Prueba de LCD	Para probar automáticamente el efecto de visualización de la pantalla LCD mostrando a todo color, blanco puro y negro puro para verificar si la pantalla muestra los colores normalmente.
Prueba de voz	Para probar automáticamente si los archivos de audio almacenados en el dispositivo están completos y la calidad de voz es buena.
Prueba del sensor de huellas dactilares	Para probar el sensor de huellas digitales presionando un dedo en el escáner para verificar si la imagen de la huella digital adquirida es clara. Cuando presiona un dedo en el escáner, la imagen de la huella digital se mostrará en la pantalla.
Cara de prueba	Para probar si la cámara funciona correctamente, verifique las imágenes tomadas para ver si son lo suficientemente claras.
Prueba de reloj RTC	Para probar el RTC. El dispositivo prueba si el reloj funciona con normalidad y precisión con un cronómetro. Para el cronómetro, toque en la pantalla para iniciar el conteo y toque nuevamente para detener el conteo.

17 Información del sistema

- Sobre el **Menú principal,** grifo **Información del sistema** para ver el estado del almacenamiento, la información de la versión del dispositivo, etc.





Función descriptiva

Nombre de la función	Descripción
Capacidad del dispositivo	Muestra el almacenamiento de usuario del dispositivo actual, el usuario administrador, la contraseña, la huella digital, el almacenamiento de rostros, el almacenamiento de credenciales, los registros de asistencia, las fotos de listas negras y de asistencia y las fotos de los usuarios.
Información del dispositivo	Muestra el nombre del dispositivo, el número de serie, la dirección MAC, el algoritmo de huellas dactilares, el algoritmo facial, la información de la plataforma, la información de la versión, el fabricante y la fecha de fabricación.
Información de firmware	Muestra la versión de firmware y otra información de versión del dispositivo.

Apéndice 1 Declaración sobre el derecho a la privacidad

Queridos clientes:

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

Declaramos que:

1. Todos nuestros dispositivos civiles de reconocimiento de huellas dactilares capturan solo características, no imágenes de huellas dactilares, y no involucran protección de privacidad.
2. Ninguna de las características de la huella dactilar que capturamos se puede utilizar para reconstruir una imagen de la huella dactilar original y no implica la protección de la privacidad.
3. Como proveedor de este dispositivo, no asumiremos ninguna responsabilidad directa o indirecta por las consecuencias que puedan resultar de su uso de este dispositivo.
4. Si desea disputar cuestiones de derechos humanos o privacidad relacionados con el uso de nuestro producto, comuníquese directamente con su distribuidor.

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

Nota:

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

1. No habrá arresto, detención, registro o infracción ilegal de personas;
2. La dignidad personal está relacionada con la libertad personal y no debe ser violada;
3. No se puede violar la casa de un ciudadano;
4. El derecho a la comunicación de un ciudadano y la confidencialidad de esa comunicación están protegidos por la ley.

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

Apéndice 2 Operación ecológica

El "período operativo ecológico" del producto se refiere al período de tiempo durante el cual este producto no descargará ninguna sustancia tóxica o peligrosa cuando se use de acuerdo con los requisitos previos de este manual.

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

Sustancias peligrosas o tóxicas y sus cantidades

Componente Nombre	Sustancia / elemento peligroso / tóxico					
	Plomo (Pb)	Mercurio (Hg)	Cadmium (Cd)	Polibrominato cromo (Cr6 +)	hexavalente Polibromado d Bifenilos (PBB)	Éteres de difenilo (PBDE)
Resistencia de chip	×	○	○	○	○	○
Condensador de chip	×	○	○	○	○	○
Inductor de chip	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
ESD componente	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Empulgueras	○	○	○	×	○	○

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

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

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

Green Label

Edificio ZK, Wuhe Road, Gangtou, Bantian, Buji Town, Longgang

District, Shenzhen China 518129 Tel: + 86755-89602345

Fax: +86755-89602394