MANUAL DE USUARIO

G3

Versión 1.2

Green Label

Acerca de este Manual

• Este documento describe las funciones del menú, y la interfaz del usuario de la serie de productos con reconocimiento del patrón venoso de los dedos. Las funciones marcadas con * son opcionales en algunos dispositivos.

• Para obtener información no consignada en este documento, por favor consulte el manual de instalación, la guía rápida o al personal técnico de su región.

Aviso importante

Primero que todo queremos agradecerle por haber adquirido este producto; antes de utilizarlo, por favor lea este manual detenidamente. Le recordamos que el uso adecuado del equipo ayudará a mejorar el rendimiento y la velocidad de verificación.

Nota de privacidad

Sin el previo consentimiento de nuestra empresa, ningún individuo tiene permitido extraer o copiar el contenido de este manual de manera parcial o total, ni distribuirlo en ningún formato.

El producto descrito en el manual tal vez incluye software cuyos derechos de autor son compartidos por los licenciantes incluyendo nuestra empresa. Con excepción de la autorización del titular correspondiente, ningún individuo puede copiar, distribuir, revisar, modificar, extraer, descompilar, desensamblar, desencriptar, invertir ingeniería, transferir o sublicenciar el Software ni realizar otros actos de violación de los derechos de autor, pero se excluyen las limitaciones aplicadas por la ley.

Términos y condiciones

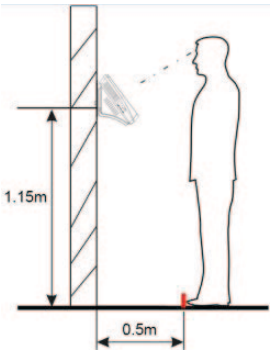
Debido a la constante renovación de productos, la empresa no puede garantizar que el artículo actual consista en su totalidad con la información consignada en este manual. Por favor disculpe los inconvenientes causados debido a los cambios hechos sin notificación. Nos reservamos los derechos finales de modificación e interpretación.

Contenido

Notas de orientación

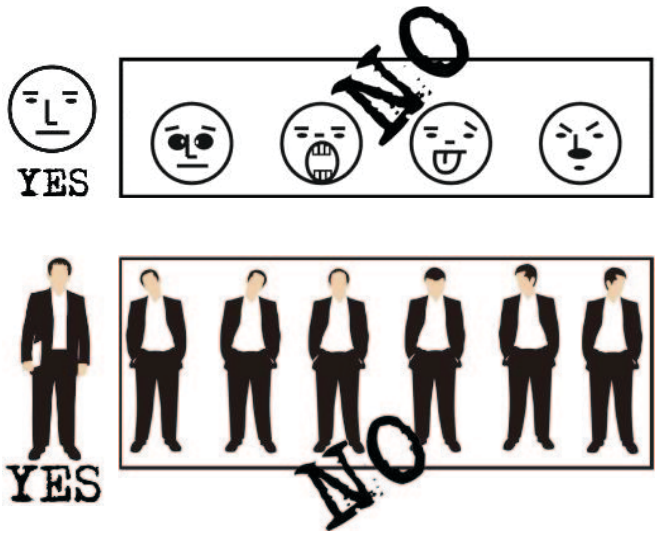
1.1 Postura y expresión facial

• Posición Recomendada



✓La distancia entre una persona y el dispositivo se recomienda que sea de 0,5 metros (rango de altura aplicable a partir de 1.5-1.8 metros) .La distancia puede ajustarse basándose en el efecto de la imagen facial capturada por el dispositivo..

• Expresión facial y postura



Nota: Durante el enrolamiento y la verificación, mantenga la expresión facial y la postura natura

Notas de orientación

1.2 Registro y Verificación

Durante el registro, se requiere ajustar la parte superior del cuerpo para colocar de forma correcta los ojos en el recuadro verde de la pantalla.

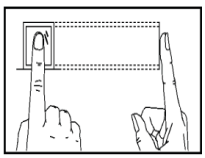
Durante la verificación, se requiere colocar su rostro en el centro de la pantalla y ajustar su cara en el marco verde.

Es recomendable colocar el rostro en el centro de la pantalla y enfocar los ojos dentro del cuadro verde según el símbolo del dispositivo.

1.3 Método para colocar la huella digital

Se recomienda utilizar el dedo índice, dedo medio o el dedo anular para registrar las huellas digitales; evitar el uso del pulgar o el dedo meñique.

1. Forma correcta para presionar la huella digital:



Coloque el dedo en forma horizontal; La huella debe estar firme, de frente y centrada en el lector de huellas.

2. Ubicación incorrecta:

Cuando la huella se encuentra muy cerca o sobre los límites del lector, cuando el dedo inclinado hacia un lado o cuando se presiona sólo una parte de la huella.

Notas de orientación

Nota: Utilice el método correcto de colocación de las huellas digitales para el registro y la verificación. Nuestra empresa no asume la responsabilidad por el mal desempeño de verificación causado por la operación incorrecta del usuario. Los derechos a la interpretación final y modificación están reservados.

1.4 Uso de la pantalla táctil

Puede tocar la pantalla táctil, o toque y deslice usando la yema del dedo. Al tocar la pantalla con la punta del dedo o la uña puede afectar el uso.

Las manchas o el polvo pueden afectar el funcionamiento de la pantalla táctil. Por lo tanto, trate de mantener la pantalla limpia y libre de polvo.

1.5 Interfaz inicial

Cuando el dispositivo está encendido, pulse el interruptor de encendido en el lado izquierdo del dispositivo y espere un minuto. Se mostrará la interfaz inicial como se muestra a continuación.

Notas de orientación

Nota:

• El estado de asistencia incluye entradas, salidas, salidas a descansos, entradas de descansos, retardos, horas extras y salidas tempranas.

• Se puede cambiar el estado del estatus tocando la pantalla principal donde no haya ningún ícono.

Puede pulsar una tecla de acceso directo para seleccionar el estado actual de asistencia, el cual se mostrará verde. Para más detalles, consulte 8.5 Accesos directos.

• Toque para entrar a la interfaz del menú principal, por favor verifique la administración cuando se haya registrado.

• Toque para entrar a la interfaz de verificación 1:1 e introduzca el ID de usuario. Para más detalles, consulte 1.8 Métodos de verificación.

Notas de orientación

1.6 Iconos de estado

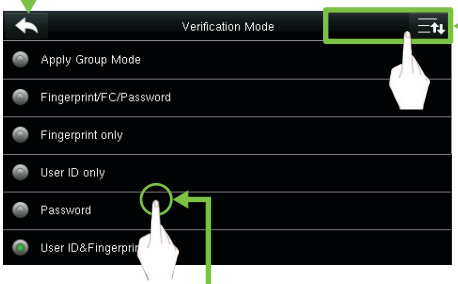
Íconos de estado	Nombre	Descripción
Los íconos de estado indican si se encuentra dentro de la cobertura de red móvil, las barras verdes indican la fuerza de la señal.		
	Señal Móvil	**G:** Indica que la actual red móvil es la red GPRS*; con la cual, el dispositivo tiene acceso a internet.
		**E:** Indica que EDGE (GSM) la red del operador está disponible, overwhich el dispositivo accede a Internet.
		**W:** Indica que la red móvil actual es la red WCDMA, overwhich el dispositivo accede a Internet.
		**H:** Indica que la red móvil actual es la red HSDPA, overwhich el dispositivo accede a Internet.
		**T:** Indica que la red móvil actual es la red TD-SCDMA, sobre la cual el dispositivo accede a la Internet.
		**1X:** Indica que la red móvil actual es la red CDMA 1X, sobre la cual el dispositivo accede a la Internet.
		**3G:** Indica que el operador de 3G UMTS(GSM) o EV-DO (CDMA) de red está disponible
		Indica que no hay una red movil
	Timbre	Indica que se ha programado un timbre
		Indica que se ha programado un timbre de desmontaje
	Ethernet	Indica que se ha establecido la conexión al Ethernet
		Indica que la Ethernet está desconectado.

Notas de orientación

	ADMS	La conexión entre el dispositivo y el servidor ADMS es exitosa.
		La conexión entre el dispositivo y el servidor ADMS es fallida.
		Los datos de comunicación ADMS se están transmitiendo.
	Mernsajes cortos	Hay mensajes públicos.
	Señal Wi-Fi	La conexión Wifi es norma

1.7 Operaciones touch

1.7.1 Operaciones Básicas



Regresar y guardar

Desplazar hacia arriba y hacia abajo.

Nota: Si la lista no tiene mucho contenido y el menú se puede visualizar por completo cuando se presiona Bajar Pág sólo una vez, se muestra aquí únicamente la tecla Bajar Pág.

Puede seleccionar una opción únicamente tocando la línea del menú en donde encuentre dicha opción y el sistema vuelve automáticamente a la interfaz anterior.

Nota: Después de registrar o modificar la información del usuario o la configuración de los parámetros, es necesario aprovechar **Retorno / Guardar** para que la configuración surta efecto. Si el tiempo de espera o no se realizan operaciones en la interfaz, el sistema vuelve a la interfaz principal sin guardar registro, modificación de información del usuario o ajustes de los parámetros.

Notas de orientación

1.7.2 Teclado

• Teclado digital

Área de visualización de contenido

Borrar entrada la anterior

Borrar entrada la anterior

Tecla de retorno

• Teclado de letras

Toque Para ver el texto hacia la izquierda y hacia la derecha.

Salir del teclado

Sugerencias de texto

Escritura texto

Borrar

Confirmar el texto y salir

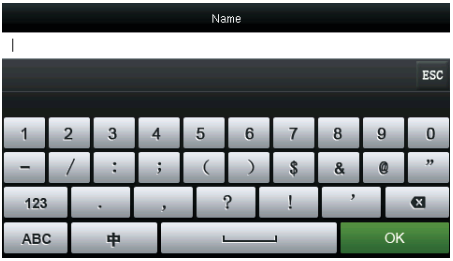
Espacio

Pulse para cambiar el teclado a Inglés

Pulse para cambiar al teclado numérico

Pulse para cambiar al teclado a mayúsculas

• Teclado de números



1.8 Métodos de Verificación

1.8.1 Verificación con Huella Digital

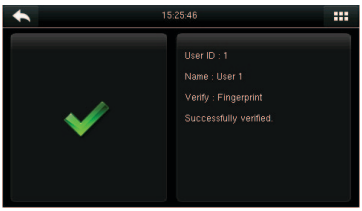
• Verificación de Huella digital 1:N

En el Método de verificación de huellas dactilares 1:N, la huella digital es recogida por el sensor y se verifica con todas las huellas digitales almacenadas en el dispositivo.

•Para entrar en el modo de verificación de huellas digitales:

El dispositivo reconoce automáticamente la cara y la huella digital. Solo tiene que pulsar el dedo en el sensor de huella digital y en dispositivo entrará en modo de autenticación de huellas

•Utilice el modo correcto de presionar la huella digital en el sensor (para obtener instrucciones detalladas, consulte 1.3 Método para colocar la huella digital.



Verificación Exitosa

Verificación Fallida

Notas de orientación

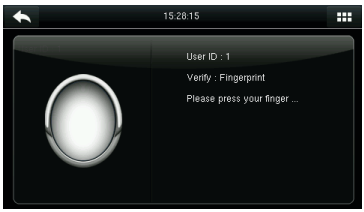
• Verificación de huella digital 1:1

En el método de verificación de huellas digitales 1:1, la huella digital es recogida por el sensor y se verifica con la huella digital correspondiente a la ID de usuario introducido previamente.

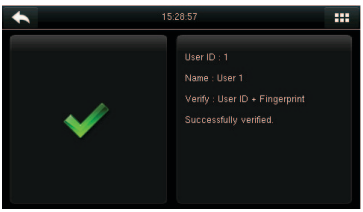
Nota: Usar este modo sólo cuando sea difícil de reconocer el dedo.

Pulse  en la pantalla para entrar al modo de verificación 1: 1

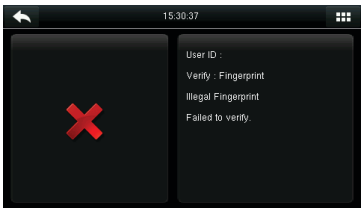
1. Ingrese su ID y presione [OK]



2. Coloque la huella digital para su verificación



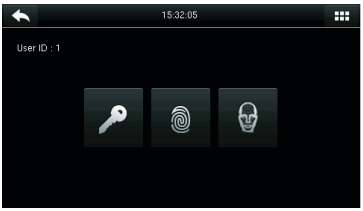
3. Verificación Exitosa



4. Verificación Fallida

Si se ha registrado con múltiples formas de verificación, la siguiente interfaz aparecerá después de introducir su ID y tocar [OK].

Notas de orientación



Toque en el icono de la huella digital para acceder a la interfaz de verificación de huellas.

Coloque dedo en el escáner de huella digital para escanear y verificar su huella. El resultado se mostrará como en la imagen.

Nota: Si ha registrado solamente su huella digital, accederá a la interfaz de verificación de huellas digitales directamente después de introducir su ID. Si se ha registrado con múltiples formas de verificación, se mostrarán los iconos de los modos de verificación registrados, como se muestra en la figura anterior con contraseña, huella digital y rostro.

1.8.2 Verificación de rostro

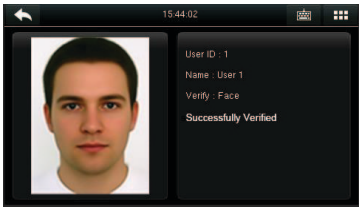
• Verificación de rostro 1:N

Compara la imagen facial capturada por la cámara con todos los datos faciales en el dispositivo.

• El dispositivo diferencia de forma automática entre los métodos de verificación de rostro y de huellas digitales. Muestre su rostro dentro de la zona de captura de la cámara (sin colocar el dedo en el escáner), y el dispositivo automáticamente realiza la detección en el modo de verificación facial.

Notas de orientación

Llevar a cabo la comparación de la forma correcta en la interfaz principal.

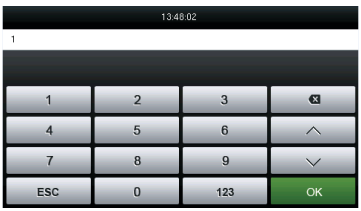


Verificación aprobada

• Verificación de rostro 1:1

Compara la imagen facial capturada con la imagen facial asociada con el ID de usuario introducido.

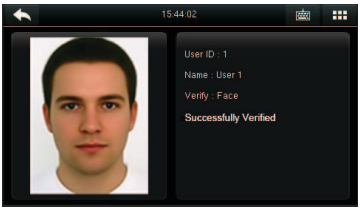
Nota: Si el dispositivo dice "No hay datos registrados" después de que el usuario introduzca el ID y pulse [OK], significa que no existe usuario correspondiente a este ID.



1.Ingrese el ID de usuario en la interfaz principal con el teclado y, a continuación, pulse [OK].

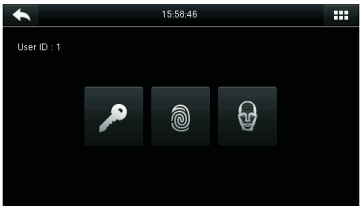
2.Comparación correcta de los rostros

Notas de orientación



3.Verification aprobada. Si la verificación falla durante 20 segundos consecutivos, el sistema vuelve a la interfaz principal.

Si se ha registrado con múltiples modos de verificación, la siguiente interfaz aparecerá después de introducir su ID y tocar [OK].



Toque en el icono del rostro para acceder a la verificación facial.

El resultado se mostrará como en la imagen.

Nota: Si ha registrado solamente su rostro, accederá a la interfaz de verificación facial directamente después de introducir su ID. Si se ha registrado con múltiples formas de verificación, se mostrarán los iconos de los modos de verificación registrados, como se muestra en la figura anterior con contraseña, huella digital y rostro.

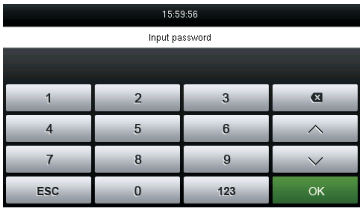
1.8.3 Verificación con contraseña

Bajo este método de verificación, la contraseña introducida se verifica con la contraseña del ID de usuario introducido.–––

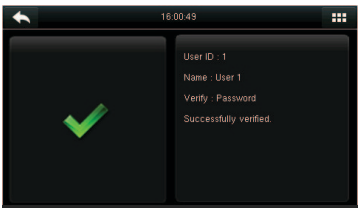
• Presione el botón de [1:1] en la interfaz inicial para entrar al modo de verificación [1:1]

Notas de orientación

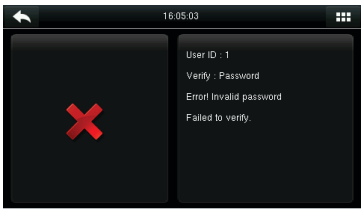
1. Introduzca el ID de usuario y presione [OK]



2. Introduzca la contraseña y pulse [OK].

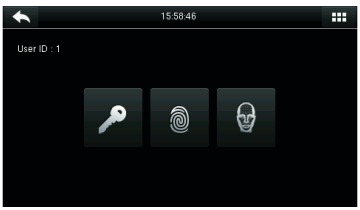


3. Verificación exitosa

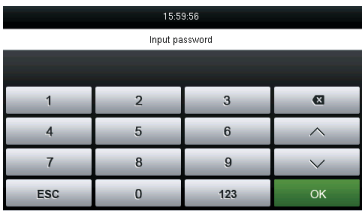


4. verificación fallida

Si se han registrado varios modos de verificación, la siguiente interfaz aparece después de introducir su ID y presionar [OK].



Pulse en el icono de la llave para acceder a la verificación de contraseñas.



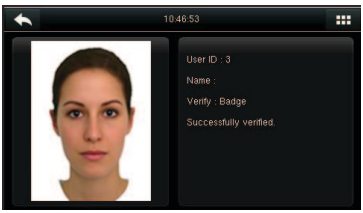
El resultado de la verificación se muestra como en la imagen.

Nota: Si se ha registrado sólo la contraseña, se accede a la interfaz de verificación de contraseña directamente después de introducir su ID. Si se ha registrado con múltiples métodos de verificación, se mostrarán los iconos de los modos de verificación registrados, al igual que la figura de arriba muestra que la contraseña, huella digital y rostro han sido registrados.

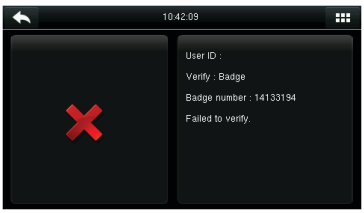
1.8.4 Verificación con tarjeta

La función de la tarjeta es opcional, solamente los productos con módulo de tarjeta incorporada están equipados con la función de verificación de tarjeta.

• Pasar la tarjeta por encima del lector de tarjetas (la tarjeta debe ser registrada por primera vez)



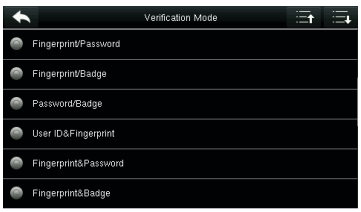
Verificación exitosa



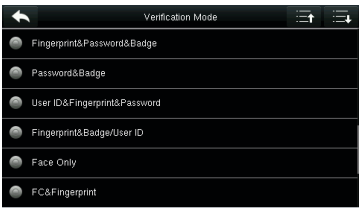
Si la tarjeta no se ha registrado "La verificación será fallida"

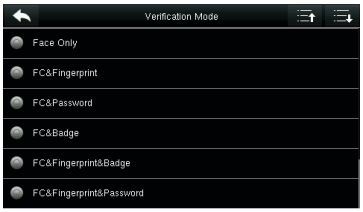
1.8.5 Multi-verificación

Con el fin de satisfacer necesidades de control de acceso ocasionales con alta seguridad y teniendo en cuenta la diversidad de control de acceso, el dispositivo ofrece una amplia gama de multi-verificaciones, que se pueden combinar según sea necesario para los usuarios individuales y grupos de usuarios. El dispositivo es compatible con 21 combinaciones de multi-verificación, como se muestra en la siguiente figura.



Notas de orientación



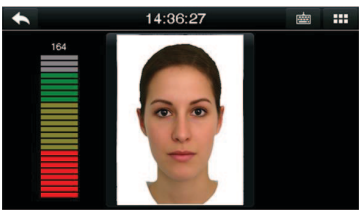


Nota: "/" Significa o, y "&" significa Y.

En el modo multi-verificación, debe registrar la información de verificación requerida, de lo contrario la verificación puede fallar. Por ejemplo, si el usuario A utiliza el registro de la huella digital pero el modo de verificación es contraseña, este usuario no pasará la verificación.

A continuación, se toma Rostro y Contraseña como ejemplo para introducir el modo multi-verificación.

• Coloque el rostro dentro del área de captura de la cámara, y el dispositivo realiza automáticamente en el modo de detección de verificación facial.



1. Verificación de rostro en proceso

2. La interfaz de entrada de la contraseña aparece después de la verificación. Introduzca la contraseña y pulse [OK]

Notas de orientación

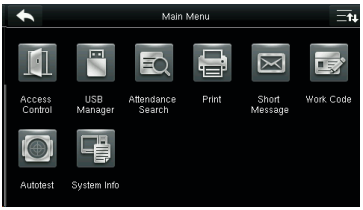
3. Verificación de rostro exitosa

4. Verificación de rosto y contaseña fallida

Nota: La multi-verificación sólo está disponible si los modos de verificación correspondientes se seleccionan durante el registro del usuario. Para más detalles consulte la sección 3.9 Configuración de los derechos de control de acceso.

Menú Principal

Cuando es dispositivo se encuentre en su interfaz inicial, presione para abrir el menú principal.



Gestión de Usuarios: Usted puede buscar en el dispositivo, la información de los usuarios registrados (ID de usuario, nombre, rol, huella digital, tarjeta, contraseña, foto del usuario); también puede realizar agregar, modificar o eliminar usuarios.

Rol del Usuario: Se utiliza para establecer los derechos de acceso de los usuarios, a los menús del dispositivo.

Comunicación: Usted puede establecer los parámetros relacionados con la comunicación del dispositivo y el PC, incluyendo la dirección IP, Puerta de enlace, Máscara de red, velocidad de transmisión, ID del dispositivo y clave de comunicación, entre otros.

Sistema: Aquí usted puede establecer la hora y fecha del dispositivo, asistencia, huella digital, cámara, reinicio y actualización USB.

Personalizar: Para cumplir con las preferencias de los clientes, con esta opción se pueden realizar cambios respecto a la pantalla, audio, sonidos y teclado.

Gestión de Datos: Con esta opción usted puede administrar la información almacenada en el dispositivo, y realizar tareas como eliminar, restaurar y hacer copia de seguridad de los datos.

Menú Principal

USB: Aquí usted puede exportar/importar la información de los usuarios y datos de asistencia almacenados en una USB, a un (o desde un) software relacionado u otro equipo de reconocimiento de huellas digitales.

Buscar Datos de Asistencia: Consulta de registros guardados en el dispositivo.

Imprimir*: Imprimir datos de asistencia

Código de Trabajo: Utilizado para identificar los diferentes tipos de trabajo, que facilita la revisión de la asistencia.

Test Automático: Este sub-menú le permite al sistema verificar que la pantalla, huella digital, voz, teclado y la hora estén trabajando correctamente.

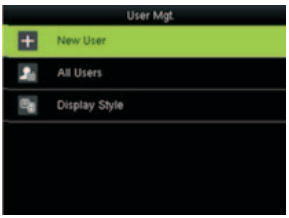
Información del Sistema: Para consultar la capacidad, información y firmware actual del dispositivo.

Nota: Si no hay ningún súper administrador está registrado en el dispositivo, cualquier persona puede acceder al menú de funciones. Después de que un administrador está configurado en el dispositivo, solo el administrador para acceder al menú de autenticación de identidad. Un usuario puede acceder al menú sólo después de la autenticación de la identidad éxito. Por razones de seguridad dispositivo, se recomienda registrar un administrador cuando se utiliza el dispositivo por primera vez. Para operaciones específicas, consulte la sección 3.3 Configurar rol del usuario

Agregar Usuario

Presione la tecla M/OK para ingresar al menú principal.

Elija la opción "Usuarios" y presione [OK].



Seleccione la opción "agregar Usuario" y presione [OK].

3.1 Agregar ID de Usuario

El dispositivo asigna automáticamente un ID iniciando desde 1 y siguiendo la secuencia. Si usted utiliza el ID asignado por el terminal, puede saltar esta sección.

En la interfaz "Nuevo Usuario" elija la opción "ID de Usuario" y presione [OK].

Nota:

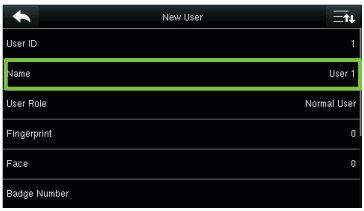
1. Por defecto, un ID de usuario contiene 1-9 dígitos. Para extender la longitud, consulte a nuestro personal de soporte técnico.

2. Durante el registro inicial, puede modificar su ID, que no puede ser modificada después del registro.

3. Si el ID ya existe se le indica que esta identificación ya se ha utilizado. Por favor, intente con ID distinto.

Agregar Usuario

3.2 Agregar Nombre de Usuario



1. Seleccione **Nuevo Usuario**

2. Introduzca su nombre y pulse OK para guardar y volver. El registro del nombre se ha completado.

Nota: Por defecto, un nombre de usuario contiene 1-12 caracteres.

Para más detalles, consulte la sección 1.7.2 Teclado

3.3 Configurar Rol de Usuario

Hay dos tipos de roles otorgados respectivamente a dos tipos de usuarios: usuario y administrador.

Usuario: Sólo se conceden los derechos de verificación, rostro, huella digital o contraseña.

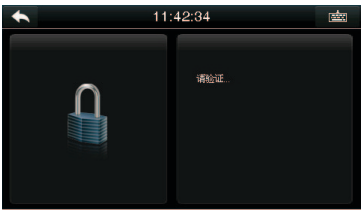
Administrador: Se ha concedido el acceso al menú principal para diversas operaciones aparte de tener todos los privilegios concedidos a los usuarios.

Agregar Usuario

Presione **Rol de Usuario**

Seleccione una función de usuario. La selección de función de usuario se ha completado.

Si la función de usuario seleccionado es Superad ministrador, debe llevarse a cabo la autentificación de identidad para acceder al menú principal. El proceso de autenticación depende del modo de autenticación que el súper administrador haya registrado. El siguiente es un ejemplo de cómo acceder al menú principal como administrador por medio de reconocimiento facial.



Presione en la interfaz principal

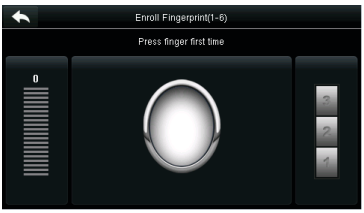
Coloque su rostro frente a la cámara para la verificación.

Podrás ingresar directamente a la interfaz del menú principal después de pasar la verificación.

Agregar Usuario

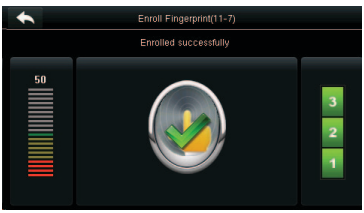
3.4 Registro de Huellas Digitales

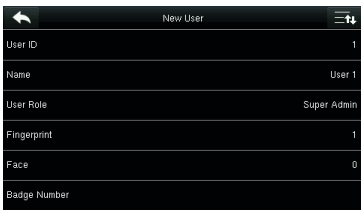
Seleccione un dedo



1. Toque para seleccionar un dedo para el registro de huellas digitales.

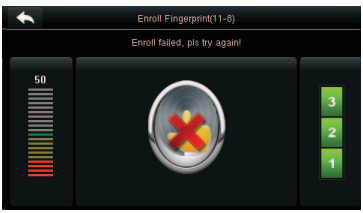
2. Coloque el mismo dedo en el escáner de huellas digitales por tres veces consecutivas.



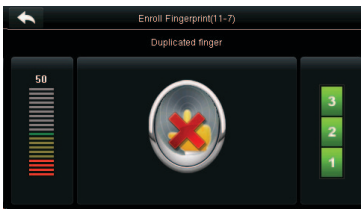


3. Interfaz de registro de huella exitoso

Si el registro de la huella digital falla, aparece el siguiente mensaje



Registro de huella fallido.
Coloque su huella nuevamente

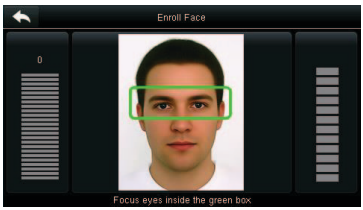


Si el dispositivo dice "huella duplicada" esta huella digital ya ha sido registrada

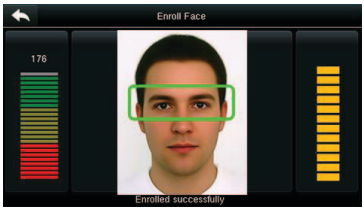
Agregar Usuario

Nota: Para registrar otra huella digital, regresa a la interfaz de nuevo usuario, coloca la huella digital y repita los pasos anteriores para seleccionar otro.

3.5 Registro de Rostro

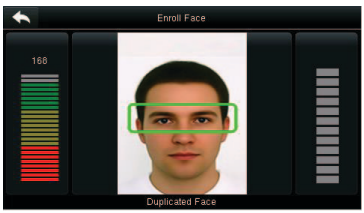


1. Siga las instrucciones y el recuadro hacia adelante y atrás colocando sus ojos en el recuadro.



2. El registro de rostro ha sido exitoso.

3. El sistema vuelve automáticamente a la nueva interfaz de usuario



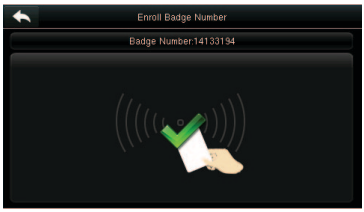
Si se duplica un registro de rostro, el sistema le dirá: "Rostro Duplicado"

Agregar Usuario

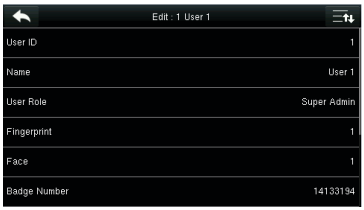
3.6 Registro de Tarjetas ID

Seleccione **Tarjetas ID**

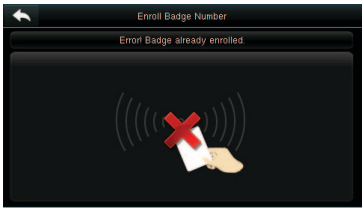
1. Coloque la tarjeta cerca del lector de huellas digitales



2. El registro de la tarjeta ha sido exitoso.



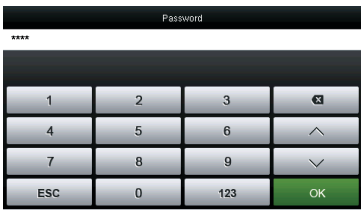
3. El sistema en automático regresa a la nueva interfaz de usuario



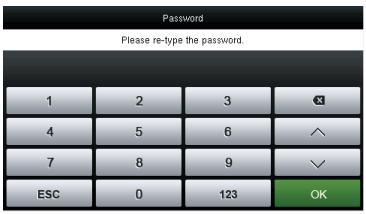
Nota: Si la tarjeta ya ha sido registrada el sistema le dirá "Error, esta tarjeta ya ha sido registrada"

3.7 Registro de Contraseña

Seleccione **Contraseña**



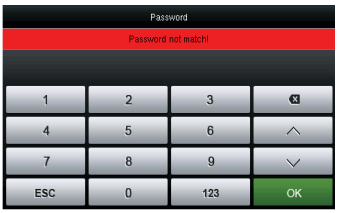
1. Ingrese su contraseña y presione OK



2. Ingrese nuevamente su contraseña y presione OK

Agregar Usuario

3. Si el registro de la contraseña es correcta, el sistema vuelve a la interfaz inicial de usuario



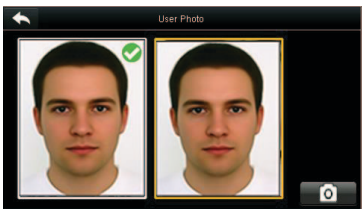
Si las contraseñas introducidas son diferentes el sistema le dirá "Las contraseñas no coinciden"

Nota: Por default, la contraseña debe contener de 1-8 dígitos

3.8 Registro de Foto

Cuando un usuario registrado con una fotografía pasa la verificación, se muestra la fotografía en la pantalla.

Seleccione **Foto de Usuario**



Seleccione el ícono de la cámara para tomar la foto.

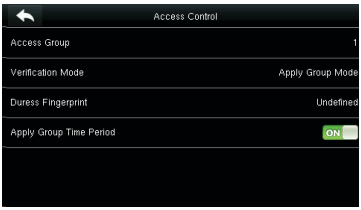
Cuando la fotografía se ha tomado, el sistema vuelve a la interfaz de usuario.

3.9 Ajustes de Derechos de Control de Acceso

Se puede establecer a qué grupo pertenece un usuario, el modo de verificación de acceso, registrar una huella de amago o la función de período de tiempo del grupo. Por default, el permiso de desbloqueo se concede a los usuarios de nuevo ingreso.

Agregar Usuario

Seleccione **Control de Acceso.**

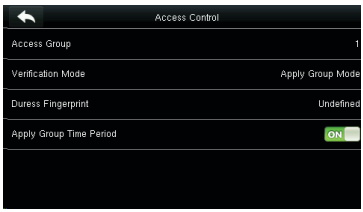


3.9.1 Grupos de Acceso

Grupo de Acceso: Seleccione el grupo a pertenecer. De forma predeterminada, un usuario recién inscrito pertenecerá al grupo uno.

Seleccione **Grupos de Acceso**

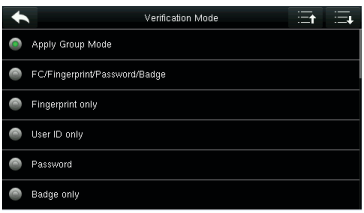
Introduzca el grupo de pertenencia y pulse OK



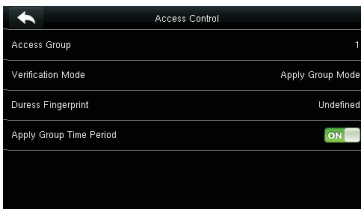
El sistema regresa a la interfaz de control de acceso.

3.9.2 Modo de Verificación

Seleccione **Modo de Verificación**



Seleccione el modo de verificación



El sistema automáticamente regresa a la interfaz de control de acceso

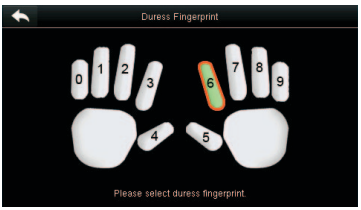
Agregar Usuario

Nota: Un usuario puede seleccionar **Aplicar modo de grupo**, es decir, el usuario puede ser verificado utilizando el modo de verificación del grupo al que pertenece este usuario, o mediante el uso de un modo de verificación individual. Para más detalles sobre la configuración del grupo, consulte la sección 10.4 Configuración de grupos de acceso.

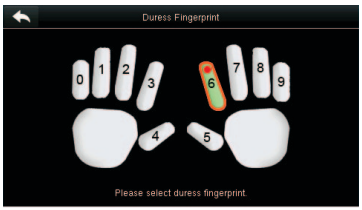
3.9.3 Huella de Amago

Una huella digital registrada en el dispositivo registrada especialmente como una huella digital de amago. En cualquier caso, se genera una alarma de amago cuando una huella digital coincide con una huella digital de amago. Después de una huella digital de amago se cancela, la huella digital no se elimina y el dedo correspondiente todavía se puede utilizar para la comparación normal.

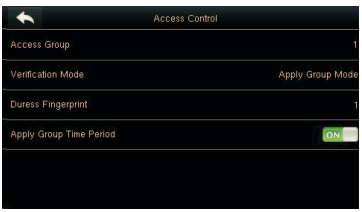
Seleccione **Huella de amago**



1. Seleccione la huella de amago



2. Cuando la selección se haya realizado correctamente, pulse el botón Volver



3. El sistema regresa a la interfaz de control de acceso

Nota: 1. La huella de amago seleccionada debe ser una huella digital registrada.

2. Si no desea utilizar la huella digital de amago, puede acceder al mismo menú durante la edición de usuario y cancelar la huella de amago.

Agregar Usuario

3.9.4 Periodos de Tiempo Aplicados a Grupos

Elija si desea aplicar el período de tiempo de grupo para este usuario, La opción sí viene activada de forma predeterminada. Si no se aplica el periodo de tiempo de grupo, es necesario establecer el tiempo de desbloqueo para este usuario. En este momento, el período de tiempo de este usuario no afecta el periodo de tiempo de cualquier otro miembro de este grupo.

Cuando se haya establecido el tiempo de desbloqueo para este usuario, presione la tecla **Aplicar periodo de tiempo de grupo**

1. Seleccione Periodo de Tiempo 1

2. Introduzca el número del periodo de tiempo y pulse OK

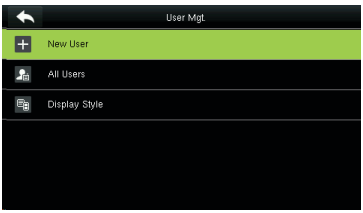
3. Seleccione periodo de tiempo 2 y 3 de la misma manea, e introduzca los numeros de perioso de tiempo

Nota: Un total de 50 periodos de tiempo se pueden establecer para cada usuario. Para más detalles consulte 10.2 Configuración de Horario

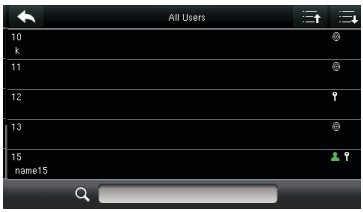
Gestión de Usuarios

Nota: Después de que se han registrado los datos anteriores, presione para volver a la interfaz de usuario. Para modificar los datos registrados, presione el menú correspondiente para el nuevo registro. Para guardar los datos que fueron nuevamente registrados, presione . Si el menú se deja en espera por un periodo largo de tiempo el sistema vuelve a la interfaz principal, y la información registrada no se guarda.

Presione **Gestión de Usuarios** en la interfaz del menú principal.



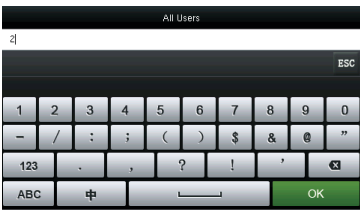
Seleccione **Todos los Usuarios**



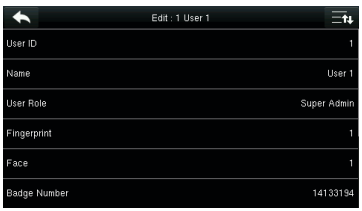
Mostrará la interfaz de la opción **Todos los Usuarios**

Nota: Los usuarios están ordenados por nombre, si un usuario es marcado por el símbolo indica que él es el súper administrador.

4.1 Buscar un Usuario



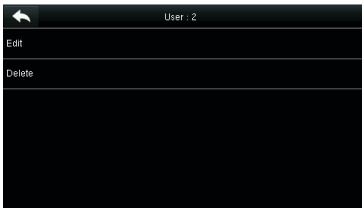
Pulse en la barra de búsqueda del menú de usuarios e introduzca una palabra clave.



El sistema en automático mostrará los usuarios relacionados con la palabra clave.

Nota: La palabra clave puede ser el ID, el nombre, el apellido o el nombre completo.

4.2 Editar un Usuario



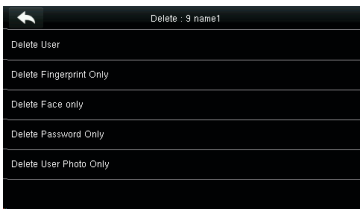
Elija un usuario de la lista y pulse **Editar**

Se mostrará la interfaz de **Editar Usuario.**

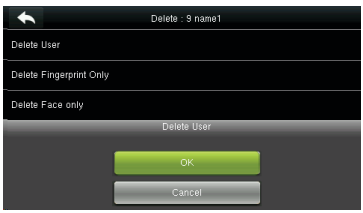
Nota: La operación para editar un usuario es la misma que la de agregar un usuario a excepción de que el ID de usuario no puede ser modificado en la edición de usuario.

4.3 Eliminar un Usuario

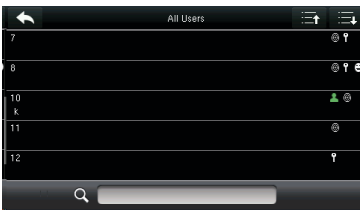
Elija un usuario de la lista y pulse **Eliminar**



Se mostrará la interfaz de **Editar Usuario** (Deslice hacia abajo para ver más información)



Seleccione la información de usuario que desea eliminar y pulse OK



El usuario se elimina con éxcito y ya no aparece en la lista

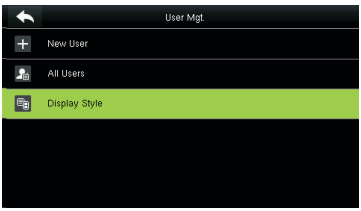
Gestión de Usuarios

Nota:

1. Cuando va a eliminar un usuario, puede elegir borrar información parcialmente como la huella o los privilegios únicamente. Si selecciona **Eliminar Usuario**, toda la información será eliminada.

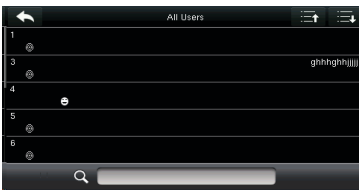
2. Después de que los privilegios del súper administrador son eliminados, el súper administrador se convierte en un usuario común, sin privilegios de súper administrador.

4.4 Estilo de Visualización

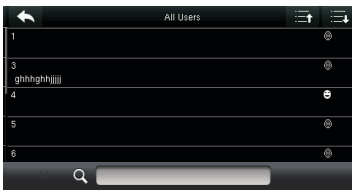


1. Presione **Estilo de Visualización** en la interfaz de usuario

2. El estilo por default es línea simple



3. La figura superior muestra todos los usuarios en el estilo de línea múltiple



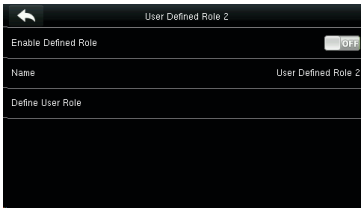
4. La figura superior muestra todos los usuarios en el estilo de línea mixta

Rol de Usuario

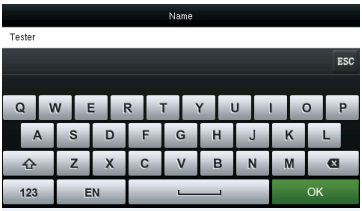
Configuración de derechos de usuario para operar el menú (como máximo 3 roles puedes ser configurados).

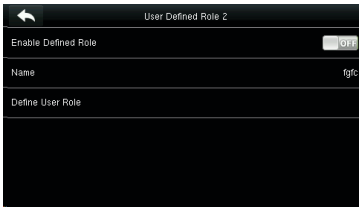
Seleccione **Rol de Usuario** en la interface del menú principal.

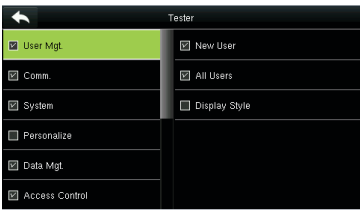
1. Seleccione cualquier elemento para establecer un papel definido



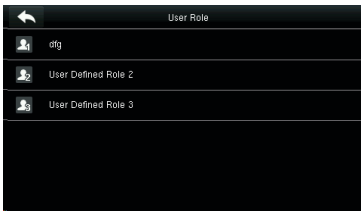
2. Toque habilitar la definición de rol







5. Pulse **Definir Rol de Usuario** para asignar privilegios al rol.



6. La definición del rol se ha completado

La asignación de privilegios se ha completado. Pulse

Ajustes de Comunicación

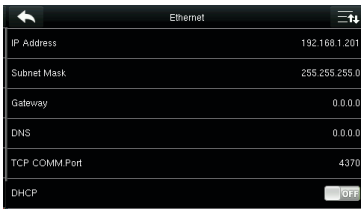
Incluyendo parámetros de Ethernet, tales como dirección IP, etc., comunicación serial, conexión para PC, ADMS y la configuración de Wiegand.

Pulse **[Comunicación]** en la interfaz del menú principal.

6.1 Ethernet

Cuando el dispositivo necesita comunicarse con una PC usando Ethernet, es necesario configurar los ajustes de red.

Toca **Ethernet** en la interfaz de **Ajustes de Comunicación**



Dirección IP: La Dirección IP predeterminada es 192.168.1.201, y puede ser modificada, de ser necesario; pero no puede ser la misma que la del PC.

Máscara de Subred: La Máscara de Subred predeterminada es 255.255.255.0, y puede ser modificada, de ser necesario.

Puerta de Enlace: La puerta de enlace predeterminada es 0.0.0.0 y puede ser modificada, de ser necesario.

Ajustes de Comunicación

DNS: El servidor DNS predeterminado es 0.0.0.0 y puede ser modificado, si es necesario.

Puerto de Comunicación TCP: El puerto predeterminado es 4370 y puede ser modificado, de ser necesario.

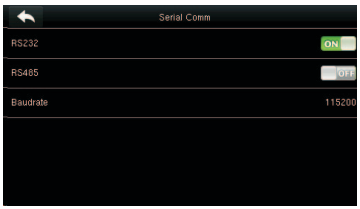
DHCP: Protocolo de Configuración Dinámica de Host (por sus siglas en inglés) es utilizado por un servidor para distribuir direcciones IP dinámicas a clientes en una red. Si el DHCP está activado, la dirección IP no puede ajustarse manualmente.

Barra de estado: Utilizado para definir si mostrar o no los iconos de red en la interfaz principal.

6.2 Comunicación Serial

Para establecer comunicación con el dispositivo a través del puerto serial (RS232/ RS485), es necesario configurar los ajustes del puerto serial.

Toque **Comunicación Serial** en la interfaz de **Ajustes de Comunicación**.



RS232: Para comunicarse con el dispositivo a través de un puerto serial RS232.

RS485: Para comunicarse con el dispositivo a través de un puerto serial RS485.

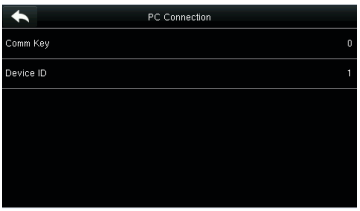
Ajustes de Comunicación

Velocidad de Baudios: La velocidad de comunicación con la PC. Hay cinco opciones: 115200 (predeterminada), 57600, 38400, 19200 y 9600. Entre más alta la velocidad, la comunicación será más rápida, pero también menos confiable o estable. En general, se puede usar una velocidad de baudios alta cuando la distancia de comunicación es corta; cuando la distancia es larga, es más fiable elegir una velocidad de baudios más baja.

6.3 Conexión a la PC

Para mejorar la seguridad de los datos, es necesario establecer una contraseña de conexión entre el dispositivo y la PC. La contraseña de conexión se utiliza cuando el Software de PC se conecta al dispositivo para leer los datos.

Toque **Conexión a la PC** en la interfaz de Ajustes de **Comunicación.**



Clave de Comunicación: La contraseña predeterminada del sistema es 0 (no hay contraseña) pero puede ser establecida. Después de establecerla, la contraseña debe ser ingresada en el software para la comunicar con el dispositivo. El sistema soporta contraseñas de 1 a 6 dígitos.

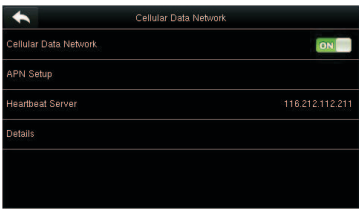
ID del Dispositivo: El número de identidad del dispositivo. Puede tomar valores entre 1-254. Si el método de comunicación RS232/RS485 es utilizado, este ID necesita ser ingresado en la interfaz de comunicación del software.

Ajustes de Comunicación

6.4 Red de Datos Móviles *

Cuando se requiere conectar el dispositivo a una red telefónica, asegúrese de que el dispositivo se encuentra dentro de la zona de cobertura de las señales móviles (GPRS/3G). Además, requerirá conocer el Nombre del Punto de Acceso (APN) y el número de acceso.

Toque **Red de Datos Móviles** en la interfaz de **Ajustes de Comunicación**



Red de Datos Móviles: Especificar si la red móvil está activada.

Configuración de APN: Para establecer la información del punto de acceso, como número de acceso, nombre de usuario y contraseña.

Servidor Heartbeat: La terminal envía periódicamente paquetes de datos ICMP (pulsos o "heartbeats") al servidor para detectar el estado de la red móvil y si la terminal está conectada a la red. Cuando la terminal está desconectada a la red, el dispositivo intenta conectarse de nuevo automáticamente. Es por esto que al establecer el servidor heartbeat usted debe asegurarse de que este sea estable y permanezca en línea por mucho tiempo.

Nota: Generalmente, el cliente puede establecer la dirección del servidor heartbeat igual que la dirección del servidor ADMS.

Detalles: Se muestra información sobre la conexión de red móvil, como modo de red, operador, dirección IP, datos recibidos y datos enviados.

Ajustes de Comunicación

6.4.1 Configuración APN

Toque **Configuración APN** en la interfaz de **Red de Datos Móviles**.

APN: Nombre del Punto de Acceso (Por sus siglas en inglés), proporcionado por el operador. No es soportado en la red CDMA.

Número de Marcación: Número de la red de datos móviles.

Nombre de Usuario y Contraseña: Para verificar si el usuario tiene los privilegios para usar esta red.

6.4.2 Detalles

Toque **Detalles** en la interfaz de Red de Datos Móviles.

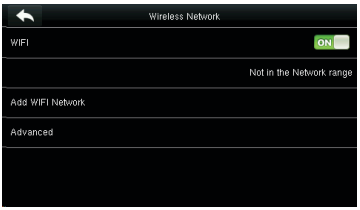
Se muestra la información de la conexión del dispositivo.

Ajustes de Comunicación

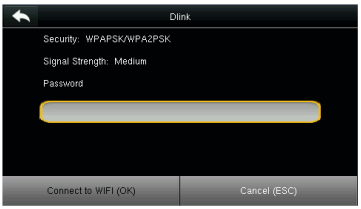
6.5 Configuración Wi-Fi *

Wi-Fi es la abreviación de Wireless Fidelity (Fidelidad inalámbrica). El dispositivo proporciona un módulo Wi-Fi, el cual puede estar integrado a la carcasa del dispositivo o puede conectarse externamente, de forma que se habilite la transmisión de datos a través de Wi-Fi y se establezca un ambiente de red inalámbrica.

El Wi-Fi viene habilitado en el sistema de forma predeterminada. Si no se necesita usar la red Wi-Fi, puede deshabilitarlo presionando el botón **ON.**



Cuando el Wi-Fi esté habilitado, toque la red encontrada



Toque el cuadro de entrada de texto para introducir la contraseña y luego toque **Conectar a Wi-Fi (OK)**

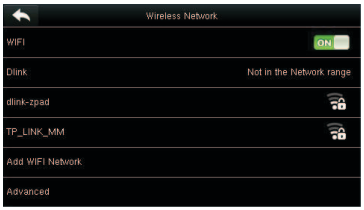
Estableciendo Conexión

Si la conexión es exitosa, se muestra el símbolo de Wi-Fi en la barra de íconos.

Ajustes de Comunicación

6.5.1 Agregar Red Wi-Fi

Si la red Wi-Fi a la que desea conectarse no aparece en la lista, puedes agregarla de forma manual.



Toque **Bajar Página** y luego **Agregar Red Wi-Fi.**

Introduzca los parámetros de la red Wi-Fi (la red agregada debe existir)

Después de agregar la red, encuentre dicha red en la lista y conéctese a ella.

6.5.2 Opciones Avanzadas

Aquí se establecen los parámetros de la red Wi-Fi.

DHCP: Protocolo de Configuración Dinámica de Host (por sus siglas en inglés) el cual se involucra en asignar direcciones IP dinámicas a clientes de red.

Dirección IP: Dirección IP de la red Wi-Fi.

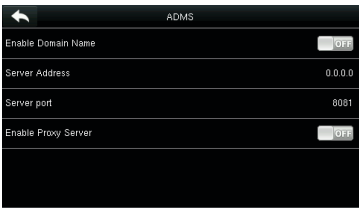
Máscara de Subred: Máscara de Subred de la red Wi-Fi.

Puerta de Enlace: Puerta de enlace de la red Wi-Fi.

Ajustes de Comunicación

6.6 Configuración ADMS

Configuraciones para hacer la conexión con el servidor ADMS. Toque Conexión a la PC en la interfaz de **Ajustes de Comunicación**



Habilitar Nombre del Dominio: Cuando esta función está activada, el nombre del dominio se usará en el formato "http://..." por ejemplo: http://www.XXX.com, donde XXX es el nombre del dominio. Cuando la función está desactivada, escriba el formato de la dirección IP en XXX.

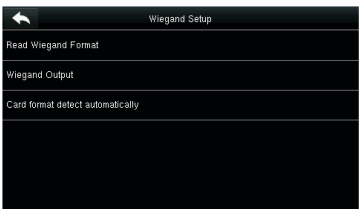
Dirección de Servidor: Dirección IP del servidor ADMS.

Puerto del Servidor: Puerto usado por el servidor ADMS.

Habilitar Servidor Proxy: Para habilitar el proxy, por favor introduzca la dirección IP y número de puerto del servidor proxy.

6.7 Configuración Wiegand

Para establecer los parámetros de la salida Wiegand, toque **Configuración Wiegand** en la interfaz de Ajustes de Comunicación.



Ajustes de Comunicación

6.7.1 Lectura de Formato Wiegand.

Seleccione el formato wiegand que coincida con el módulo de tarjeta del dispositivo. Al usarse un formato wiegand unificado, los números de las tarjetas se pueden leer correctamente. Puede elegir entre los formatos IntWiegand26, IntWiegand26a, IntWiegand34 o IntWiegand34a, de forma que las tarjetas leídas por el dispositivo estén en el formato adecuado.

Formato Wiegand	Descripción
IntWiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Está compuesto de 26 números binarios, con el bit 1 siendo el bit de comprobación de paridad par para los bits 2-13, y el bit 26 siendo el bit de comprobación de paridad impar para los bits 14-25. Los bits 2-15 corresponden al número de tarjeta.
IntWiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Está compuesto de 26 números binarios, con el bit 1 siendo el bit de comprobación de paridad par para los bits 2-13, y el bit 26 siendo el bit de comprobación de paridad impar para los bits 14-25.Los bits 2-9 corresponden al código de área mientras que los bits 10-15 corresponden al número de tarjeta.
IntWiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Está compuesto de 34 números binarios, con el bit 1 siendo el bit de comprobación de paridad par para los bits 2-17, y el bit 34 siendo el bit de comprobación de paridad impar para los bits 18-33. Los bits 2-15 corresponden al número de tarjeta.

IntWiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO Está compuesto de 34 números binarios, con el bit 1 siendo el bit de comprobación de paridad par para los bits 2-17, y el bit 34 siendo el bit de comprobación de paridad impar para los bits 18-33. Los bits 2-9 corresponden al código de área mientras que los bits 10-15 corresponden al número de tarjeta.

Nota: C Significa "Número de Tarjeta", E significa "Comprobación de paridad par", O significa "Comprobación de paridad impar".

Nota: Esta función está disponible para dispositivos de tarjetas ID, pero no para dispositivos de tarjetas MF.

6.7.2 Salida Wiegand

Toque Salida Wiegand en la interfaz de Configuración Wiegand.

Formato Wiegand: Los usuarios pueden elegir entre los formatos wiegand incorporados en el sistema. Aunque se soportan varios formatos, el formato real está determinado por los Bits de Salida Wiegand.

Bits de Salida Wiegand: Número de bits de los datos wiegand. Después de elegir los Bits de Salida Wiegand, el dispositivo usará este valor para encontrar el formato wiegand más adecuado en Formato Wiegand. Por ejemplo, si se selecciona el formato Wiegand26, Wiegand34a, Wiegand36, Wiegand37a o Wiegand50 en Formato Wiegand, pero se eligió 36 en los Bits de Salida Wiegand, el formato Wiegand36 tendrá efecto.

Ajustes de Comunicación

ID Fallida: Se define como el valor de salida de una verificación de usuario fallida. El formato de salida depende del Formato Wiegand seleccionado. El valor predeterminado oscila de 0 a 65535.

Código de Área: Es similar al ID del dispositivo excepto que este puede establecerse manualmente y puede repetirse en diferentes dispositivos. El valor predeterminado oscila de 0 a 256.

Amplitud de Pulso (us): La amplitud del pulso enviado por Wiegand. El valor predeterminado es 100 microsegundos, pero puede ajustarse entre 20 a 100 microsegundos.

Intervalo de Pulso (us): El valor predeterminado es 1000 microsegundos, pero puede ajustarse entre 200 a 20000 microsegundos.

Tipo de ID: El contenido de salida después de una verificación exitosa. Se puede elegir entre ID de usuario o número de tarjeta.

Definiciones de varios formatos wiegand generales:

Formato Wiegand	Descripción
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Consiste de 26 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-13, mientras el bit 26 es el bit de paridad impar para los bits 14-25. Los bits 2-15 corresponden al número de tarjeta.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consiste de 26 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-13, mientras el bit 26 es el bit de paridad impar para los bits 14-25. Los bits 2-9 corresponden al código de área mientras que los bits 10-15 corresponden al número de tarjeta.

Ajustes de Comunicación

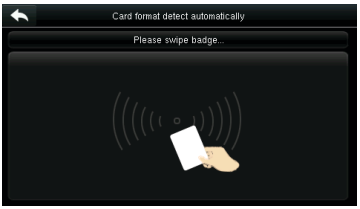
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 34 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-17, mientras el bit 34 es el bit de paridad impar para los bits 18-33. Los bits 2-25 corresponden al número de tarjeta.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 34 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-17, mientras el bit 34 es el bit de paridad impar para los bits 18-33. Los bits 2-9 corresponden al código de área mientras que los bits 10-25 corresponden al número de tarjeta.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consiste de 36 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 36 es el bit de paridad impar para los bits 19-35. Los bits 2-17 corresponden al código del dispositivo. Los bits 18-33 corresponden al número de tarjeta. Los bits 34-35 corresponden al código del fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consiste de 36 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 36 es el bit de paridad impar para los bits 19-35. Los bits 2-19 corresponden al código del dispositivo. Los bits 20-35 corresponden al número de tarjeta.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE Consiste de 37 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 37 es el bit de paridad impar para los bits 19-36. Los bits 2-4 corresponden al código del fabricante. Los bits 5-16 corresponden al código de área. Los bits 21-36 corresponden al número de tarjeta.

Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consiste de 37 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-18, mientras el bit 37 es el bit de paridad impar para los bits 19-35. Los bits 2-4 corresponden al código del fabricante. Los bits 5-14 corresponden al código del dispositivo. Los bits 15-20 corresponden al código de área. Los bits 21-36 corresponden al número de tarjeta.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste de 50 bits de código binario. El bit 1 es el bit de paridad par para los bits 2-25, mientras el bit 50 es el bit de paridad impar para los bits 26-49. Los bits 2-17 corresponden al código de área. Los bits 18-49 corresponden al número de tarjeta.
C significa número de tarjeta, **E** significa bit de paridad par, **O** significa bit de paridad impar, **F** significa código del dispositivo, **M** significa código del fabricante, **S** significa código de área.	

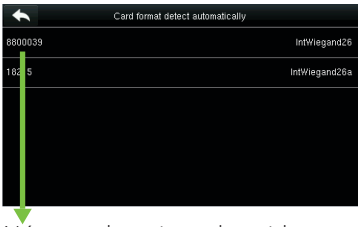
6.7.3 Detección Automática de Formato de Tarjeta

La función Detección Automática de Formato de Tarjeta tiene como objetivo asistir al usuario al detectar rápidamente el tipo de tarjeta y su formato correspondiente. El dispositivo puede leer varios formatos de tarjeta. Después de presentar una tarjeta, el sistema leerá el número de la tarjeta y comparará este número con diferentes formatos. El usuario sólo necesita elegir el formato que coincida con el número real de la tarjeta y establecer ese formato Wiegand para el dispositivo. Esta función también aplica para la función de lectura de tarjetas en lectores Wiegand auxiliares.

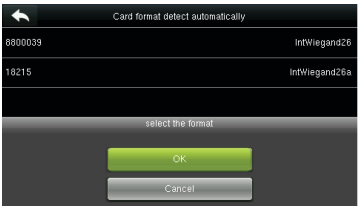
Ajustes de Comunicación



El formato Wiegand y el número de la tarjeta presentada se detectan automáticamente.



Número de tarjeta obtenido basado en el formato IntWiegand26

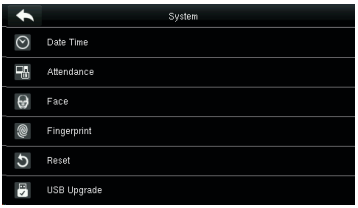


Selecciona el número que coincida con el número real de la tarjeta, el formato que le corresponda es el formato Wiegand que debe ser seleccionado para leer este tipo de tarjetas.

Configuración del Sistema

Establece los parámetros relacionados al sistema para maximizar el rendimiento del dispositivo.

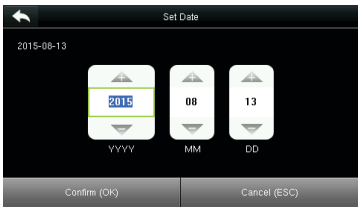
Toque **Sistema** en la interfaz del menú principal.



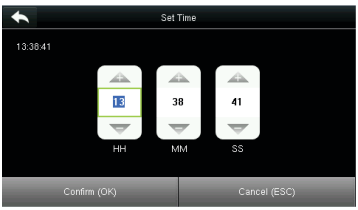
7.1 Fecha/Hora

Toque **Fecha/Hora** en la interfaz principal del sistema.

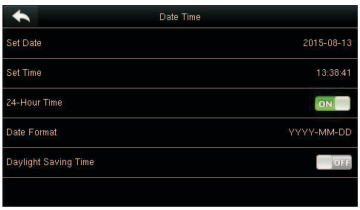
Toque **Establecer Fecha**



Toque Subir Página o Bajar Página para establecer el año, mes y día y luego presione **Confirmar (OK).**

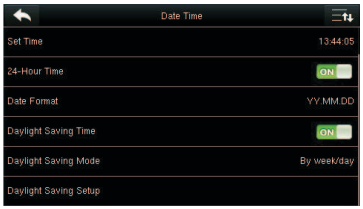


Toque Establecer Hora en la interfaz Fecha/Hora y toque Subir Página o Bajar Página para establecer la hora, minuto y segundo

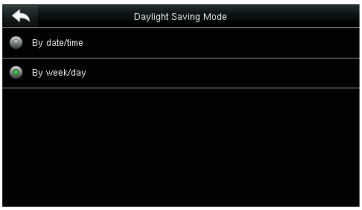


Toque Horario de 24 Horas para elegir si quiere activar este formato

Toque Formato de Fecha en la interfaz de Fecha/Hora para seleccionar el formato de visualización.



Toque Cambio de Horario para elegir si desea activar el horario de verano.

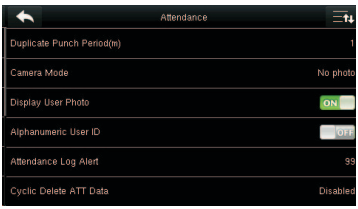


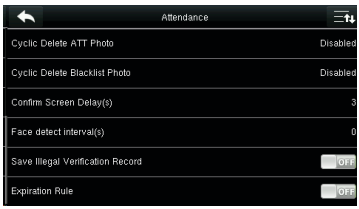
Seleccione un modo de cambio de horario.

Seleccione la fecha de inicio y fin del cambio de horario.

7.2 Asistencia

Toque Asistencia en la interfaz de Sistema.





Configuración del Sistema

Periodo de Acceso Duplicado (m): Durante un periodo de tiempo determinado (Unidad: Minutos) los registros de acceso duplicados no se guardarán en el sistema (el valor oscila de 1 a 999999 minutos).

Modo de Cámara: Sirve para establecer si se tomarán y guardarán fotos durante la verificación; aplicable a todos los usuarios. Se incluyen los siguientes 5 modos:

- No tomar Foto: No se toman fotos durante la verificación del usuario.
- Tomar foto sin guardar: Durante la verificación, se toma una foto, pero no se guarda.
- Tomar foto y guardar: Durante la verificación, se toma una foto y se guarda.
- Guardar en verificación exitosa: Se toma y guarda una foto en cada verificación exitosa.
- Guardar en verificación fallida: Se toma y guarda una foto en cada verificación fallida.

Mostrar Foto de Usuario: Para establecer si se mostrará una foto cuando un usuario verifique exitosamente. Active la función (ON) para mostrar la foto del usuario y desactívela (OFF) si no desea mostrar una foto.

ID alfanumérico de usuario: Establecer si el ID del empleado soporta el uso de letras.

Alerta por Memoria Baja: Cuando la memoria de almacenamiento restante es menor al valor establecido, el dispositivo alertará automáticamente a los usuarios sobre la cantidad de almacenamiento restante. La función puede desactivarse o establecerse a un valor de entre 1 a 9999.

Configuración del Sistema

Limpieza periódica de Eventos: La cantidad de registros de asistencia serán eliminados cada vez que se llega a la máxima capacidad de almacenamiento. La función puede desactivarse o establecerse a un valor de entre 1 a 999.

Limpieza periódica de fotos de Asistencia: La cantidad de fotos de asistencia serán eliminados cada vez que se llega a la máxima capacidad de almacenamiento. La función puede desactivarse o establecerse a un valor de entre 1 a 99.

Duración de Pantalla de Confirmación (s): El tiempo que se muestra en la pantalla la información de verificación después de un evento. El valor oscila de 1 a 9 segundos.

Intervalo de detección de rostro (s): Establecer el tiempo para realizar la detección de un rostro. El valor oscila de 0 a 9 segundos.

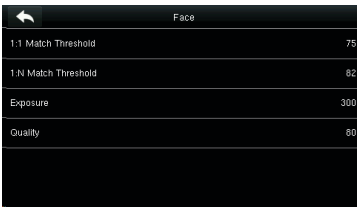
Guardar registros de verificaciones ilegales: Establecer si las verificaciones fallidas, como aquellas causadas por intentos de acceso en horario inválido o por verificaciones combinadas ilegales, se guardarán en el sistema cuando la función de control de acceso avanzado esté activada.

Reglas de Usuario Expirado: Decida si desea activar esta función. Si la activa, establezca los ajustes de expiración, que incluyen: Guardar información de usuario sin guardar registros, Guardar información de usuario y registros; y Borrar información de usuario.

Configuración del Sistema

7.3 Rostro

Toque Rostro en la interfaz de Sistema.



		Umbral de Verificación	
FRR	FAR	1:N	1:1
Alto	Bajo	85	80
Medio	Medio	82	75
Bajo	Alto	80	70

Umbral de Verificación 1:1: Bajo el método de verificación 1:1, la verificación sólo será exitosa cuando la similaridad entre el rostro a verificar y el rostro registrado del usuario sea mayor al valor establecido. El rango de valores válido es 70-120, con un valor alto resultando en un bajo FAR (Falso Error de Aceptación) y un alto FRR (Falso error de rechazo), y viceversa.

Umbral de Verificación 1:N: Bajo el método de verificación 1:N, la verificación sólo será exitosa cuando la similaridad entre el rostro a verificar y los rostros registrados sea mayor al valor establecido. El rango de valores válido es 80-120, con un valor alto resultando en un bajo FAR (Falso Error de Aceptación) y un alto FRR (Falso error de rechazo), y viceversa.

Detectar Rostro Falso: Cuando esta función esta activada, el dispositivo detecta automáticamente una cara falsa.

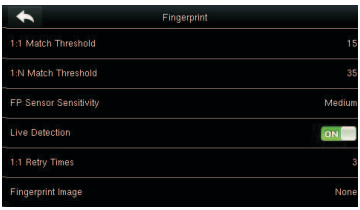
Exposición: Establece el valor de la exposición de la cámara.

Calidad: Establece el umbral de calidad para las imágenes faciales obtenidas. La terminal acepta las imágenes faciales y las procesa adoptando el algoritmo facial cuando su calidad es mayor al umbral seleccionado; de lo contrario, las imágenes son filtradas.

Nota: El ajuste incorrecto de los parámetros Exposición y Calidad pueden afectar severamente el funcionamiento de la terminal. Favor de ajustar el parámetro Exposición sólo bajo la guía del personal de servicio post-venta de nuestra empresa.

7.4 Huella Digital

Toque Huella Digital en la interfaz de Sistema.



		Umbral de Verificación	
FRR	FAR	1:N	1:1
Alto	Bajo	45	25
Medio	Medio	35	15
Bajo	Alto	25	10

Umbral de Verificación 1:1: Bajo el método de verificación 1:1, la verificación sólo será exitosa cuando la similaridad entre la huella digital a verificar y la huella registrada del usuario sea mayor al valor establecido.

Umbral de Verificación 1:N: Bajo el método de verificación 1:N, la verificación sólo será exitosa cuando la similaridad entre la huella digital a verificar y las huellas registradas sea mayor al valor establecido.

Sensibilidad del Sensor de Huellas: Se recomienda dejar el valor predeterminado "Medio". Cuando el ambiente sea seco y la detección de huellas sea lenta, puede establecer el nivel a "Alto" para aumentar la sensibilidad. Cuando el ambiente sea húmedo, haciendo difícil la detección de huellas, puede establecer el nivel a "Bajo".

Configuración del Sistema

Detección de dedo vivo: Definir si se utiliza la función anti-huellas falsas. Cuando está activada esta herramienta y se esté registrando o verificando huellas digitales; el dispositivo puede identificar las huellas las falsas, llevando al fallo de la verificación o que no se acepte la huella.

Reintentos 1:1 : Este parámetro es utilizado para establecer el número de reintentos en el caso de errores de la verificación 1:1 o verificación de contraseña debido a la ausencia de registro de la huella digital o posicionamiento incorrecto del dedo en el sensor de huellas, para prevenir operaciones reiteradas

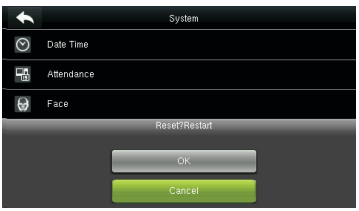
Imagen de la Huella Digital: Esta función determina si desea mostrar la imagen de la huella digital durante el registro o verificación de estas. Hay 4 opciones:

- Mostrar imagen de la huella digital sólo durante el registro.
- Mostrar imagen de la huella digital sólo durante la verificación.
- Mostrar imagen de la huella digital durante el registro y la verificación.
- No mostrar la huella digital en ningún caso.

7.5 Reestablecer Ajustes de Fábrica

Reestablece información como ajustes de comunicación o de sistema a los ajustes de fábrica.

Toque **Reestablecer Equipo** en la interfaz de Sistema.



Toque OK para confirmar el restablecimiento del sistema.

7.6 Actualización por USB

Con esta opción, se puede actualizar el firmware utilizando un archivo de actualización en un USB. Antes de realizar esta operación, asegúrese de que la unidad USB está conectada correctamente y que contiene el archivo de actualización correcto.

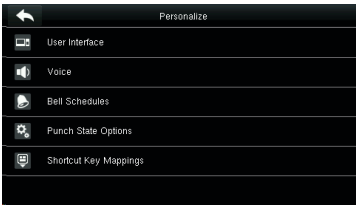
Si no hay una unidad USB conectada, el sistema arroja el siguiente mensaje cuando usted toca Actualización por USB en la interfaz de Sistema.

Nota: Si necesita el archivo de actualización, favor de contactar a nuestro soporte técnico. La actualización del firmware no es recomendable bajo circunstancias normales.

Personalizar

Realiza ajustes relacionados a la Interfaz de Usuario, Sonido, Timbre, Estado de Verificación y modificación de las teclas de atajo.

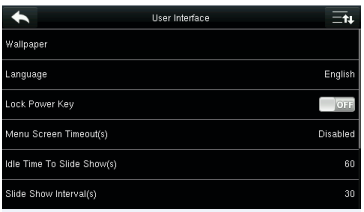
Toque **[Personalizar]** en la interfaz del menú principal.

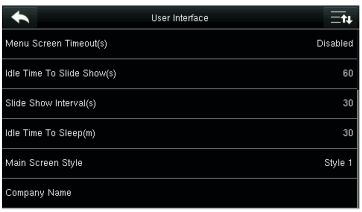


8.1 Interfaz de Usuario

Puedes personalizar el estilo de la interfaz inicial.

Toca **Interfaz de Usuario** en la interfaz de Personalizar.





Papel Tapiz: Selecciona la imagen a utilizar como fondo de pantalla.

Idioma: Seleccionar el idioma del dispositivo.

Bloquear Botón de Apagado: Con el fin de prevenir que el dispositivo se apague por error, puede activar esta función. Cuando se encuentra desactivada, el dispositivo se apagará si mantiene presionada la tecla de Encendido/Apagado por más de 3 segundos. Cuando la función se encuentre activada, la tecla de Apagado/Encendido queda deshabilitada.

Tiempo de Espera del Menú: El dispositivo vuelve automáticamente a la interfaz inicial si habiendo abierto el menú no se ha hecho ninguna operación después del periodo de tiempo seleccionado (el rango es de 60 a 99999 segundos). Esta función puede ser desactivada.

Tiempo de Espera para Diapositivas: La presentación es mostrada cuando no se estén realizando operaciones en la interfaz inicial. El rango de tiempo es de 3 a 999 segundos. Esta función puede ser desactivada.

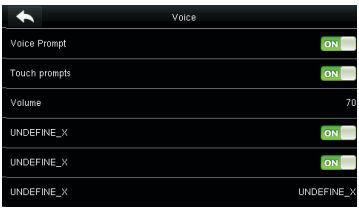
Intervalo de tiempo para Dispositivas: Este parámetro es utilizado para establecer el tiempo de duración de las diapositivas en pantalla. El rango de tiempo es de 0 a 999 segundos.

Tiempo de espera para Reposo: Esta función permite establecer el tiempo de espera del dispositivo para ingresar al modo de reposo. Usted sacar al dispositivo del modo reposo presionando cualquier tecla. El rango de espera es de 1 a 30 minutos, el tiempo preestablecido es de 3 minutos. Esta función se puede desactivar.

Estilo de la Pantalla Principal: Seleccione el estilo de la pantalla de inicio.

8.2 Voz

Toque **Voz** en la interfaz de Personalizar.



Voz: Activar o desactivar los mensajes auditivos durante la operación del dispositivo. Seleccione ON para habilitar el sonido.

Sonido de Touchscreen: Activar o desactivar el sonido de la pantalla táctil. Seleccione ON para habilitar el sonido.

Volumen: Ajuste el volumen del dispositivo.

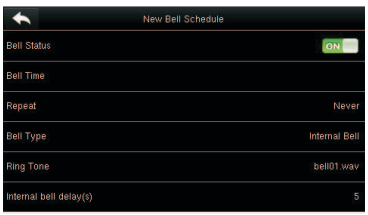
8.3 Timbre

Muchas empresas eligen utilizar un timbre para dar aviso del inicio/fin de la jornada laboral. Cuando llegue la hora programada de un timbre, el dispositivo hará sonar automáticamente el tono seleccionado durante el tiempo establecido por el usuario.

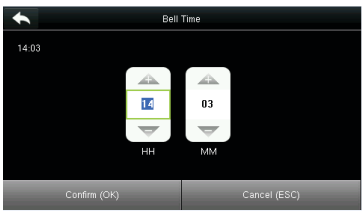
8.3.1 Agregar un Timbre

Toque **Timbre Programado** en la interfaz de **Personalizar**.

Toque **Nuevo Horario de Timbre**



Toque **Estado del Timbre** para Activar/ Desactivar ese timbre

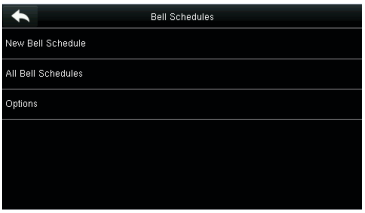


Establecer Horario de Timbre

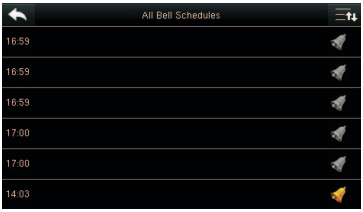
Establecer los días que el timbre se debe **Repetir**

Seleccione un **Tono** de Timbre.

Seleccione la duración del Timbre (segundos)



Regrese a la interfaz de **Timbre Programado** y toque **Horarios de Timbre**



Los timbres agregados se muestran en una lista

8.3.2 Editar un Timbre

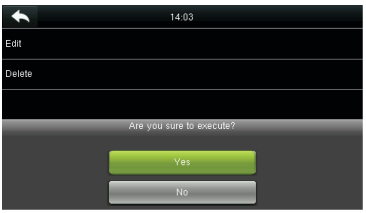
En la interfaz Horarios de Timbre, toque el timbre que desea editar.

Toque Editar

El método de edición es igual al de agregar un timbre, por lo que no se describe aquí

8.3.3 Eliminar un Timbre

En la interfaz Horarios de Timbre, toque el timbre que desea eliminar.



Toque Eliminar y selecciones "SI" para eliminar el timbre

El timbre se ha eliminado exitosamente

8.4 Estados de Asistencia

Toque Ajustes de Estado de Asistencia en la interfaz de Personalizar.

Modo de Estado de Asistencia: Esta opción es para seleccionar el Estado de Asistencia. Las siguientes opciones están disponibles:

- Apagado: El Estado de Asistencia no es utilizado. El Estado de Asistencia definido en Función queda inhabilitado.

- Modo Manual: Los Estados de Asistencia son cambiados manualmente y el Estado de Asistencia actual desaparecerá cuando transcurra el Tiempo de Espera del Estado de Asistencia.

- Modo Automático: Si un Estado de Asistencia es configurado para ser cambiado después de cierto periodo de tiempo, el Estado de Asistencia se cambiará automáticamente cuando transcurra la hora predeterminada.

- Modo Manual & Automático: La interfaz principal muestra los Estados de Asistencia que cambian automáticamente y además usted tiene la opción de cambiar el Estado de Asistencia manualmente. Un Estado de Asistencia que usted seleccione manualmente cambiará automáticamente cuando pase el tiempo de espera configurado.

- Modo Fijo Manual: Cuando el Estado de Asistencia sea cambiado manualmente, se mantendrá fijo hasta que sea cambiado manualmente de nuevo.

- Modo Fijo: Un Estado de Asistencia es siempre mostrado y no puede ser cambiado.

Tiempo de Espera del Estado de Asistencia: Especificar el tiempo límite del Estado de Asistencia mostrado en la interfaz principal.

Estado de Asistencia Requerido: Especificar si el Estado de Asistencia debe ser seleccionado durante la autenticación.

8.5 Teclas de Función

Usted puede definir Teclas de Función como Estados de Asistencia o como funciones del menú. Cuando se encuentre en la interfaz principal, oprima la Tecla de Función correspondiente para mostrar un Estado de Asistencia o para acceder a la interfaz de un menú de operaciones.

Personalizar

Toque **Teclas de Función** en la interfaz de Personalizar.

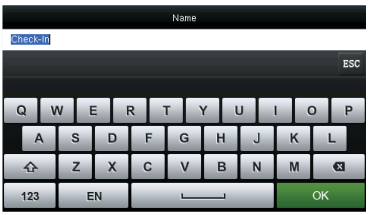
Elija la Tecla de Función a configurar (Para saber dónde se encuentran las teclas de Función, consulte la sección 1.5 Interfaz Inicial)

Se muestra la interfaz de ajustes de Teclas de Función

Establezca el Valor del Estado (0-250)

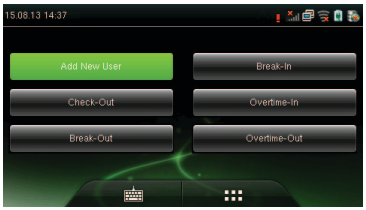
Establezca la función correspondiente para esta tecla

Elija el nombre del Estado



También puede introducir un nombre personalizado para el Estado

Personalizar



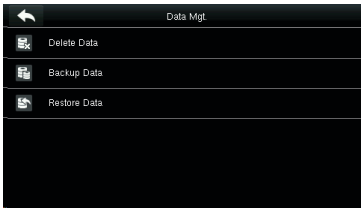
Toque la interfaz principal para verificar la Tecla de Función configurada.

Toque un Estado de Asistencia para cambiar a ese Estado, toque una función para acceder rápidamente a las configuraciones de esa función. (Por ejemplo, Toque F1 para acceder a las configuraciones de "**Nuevo Usuario**")

Gestión de Datos

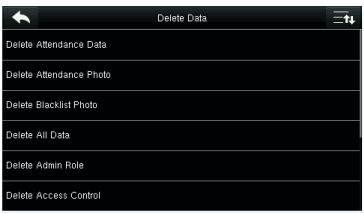
Aquí puede gestionar los datos del dispositivo, lo que incluye borrar, respaldar y restaurar los datos.

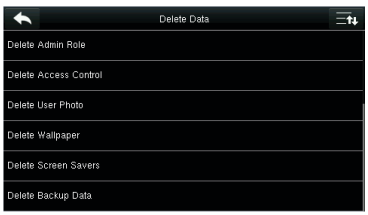
Toque **Datos** en la interfaz del menú principal.



9.1 Borrar Datos

Toque Borrar Datos en la interfaz de Datos





Borrar Eventos: Eliminar todos los datos de asistencia.

Borrar Fotos de Eventos: Eliminar todas las fotos de asistencia de los usuarios en el dispositivo.

Borrar Fotos de lista negra: Eliminar todas las fotos de lista negra en el dispositivo, que son las fotos tomadas después de verificaciones fallidas.

Borrar Todo: Eliminar toda la información de los usuarios; incluyendo huellas, imágenes faciales, registros de asistencia, etc.

Borrar Privilegio de Administrador: Cambiar todos los administradores a usuarios normales.

Borrar Fotos de Usuario: Eliminar todas las fotos de usuarios en el dispositivo.

Borrar Fondo de Pantalla: Eliminar todos los fondos de pantalla en el dispositivo.

Borrar Protectores de Pantalla: Eliminar todos los protectores de pantalla en el dispositivo.

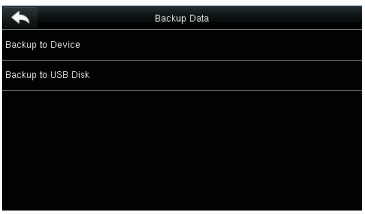
Borrar Datos de Respaldo: Eliminar los datos pertenecientes a la copia de seguridad.

Nota: Al borrar los registros de eventos, fotos de eventos o fotos de lista negra, puedes elegir Borrar Todo o Borrar por Horario. Cuando se selecciona borrar por horario, necesitas establecer el rango de fecha y tiempo que deseas eliminar.

9.2 Respaldar Datos

Aquí puede respaldar los datos del negocio o de configuración del sistema en el dispositivo o en una memoria USB.

Toque **Respaldar Datos** en la interfaz de Datos

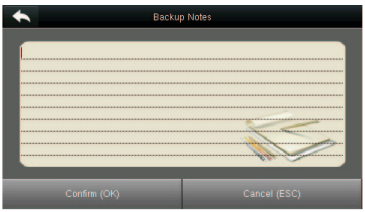


Seleccione Respaldar en el Equipo

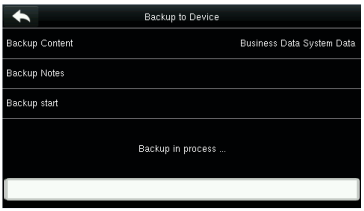
Toque Respaldar contenido

Gestión de Datos

Seleccione el contenido a respaldar



Haga notas del respaldo (Opcional)



Toque Iniciar respaldo y espere a que termine

Nota: Las operaciones de Respaldar en el Equipo son iguales a las de Respaldar en Unidad USB. Cuando se elija respaldar datos en USB, asegúrese de que la unidad USB esté conectada correctamente en el dispositivo.

9.3 Restaurar Datos

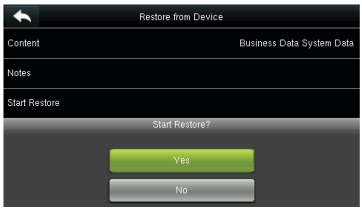
Sirve para restaurar datos guardados en el dispositivo o en un USB al dispositivo.

Toque **Restaurar Datos** en la interfaz de **Datos**

Toque Restaurar desde Equipo

Toque Contenido

Seleccione el contenido de datos que quiere restaurar



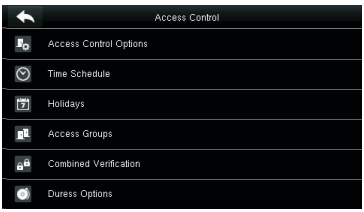
Iniciar Restauración y seleccione SI para confirmar la restauración.

Nota: Las operaciones de Respaldar en el Equipo son iguales a las de Respaldar en Unidad USB. Cuando se elija respaldar datos en USB, asegúrese de que la unidad esté conectada correctamente en el dispositivo.

Control de Acceso

.La opción Control de Acceso se usa para establecer los horarios, Días festivos, Grupos de Acceso, Verificación combinada etc., así como los parámetros necesarios para que el dispositivo controle una cerradura y otros dispositivos.

Toque **[Acceso]** en la interfaz del menú principal.



Para obtener acceso, el usuario registrado debe cumplir con las siguientes condiciones:

1.- La hora de acceso de usuario cae ya sea dentro del horario personal del usuario o el horario grupal.

2.- El grupo de usuario debe estar en el combo de acceso (cuando hay otros grupos en el mismo combo de acceso, se requiere la verificación de los miembros de esos grupos para abrir la cerradura).

En las configuraciones de fábrica, los nuevos usuarios son asignados en el primer grupo con el horario grupal por defecto y combo de acceso "1" (y se establecen en estado desbloqueado).

10.1 Opciones de Acceso

Aquí se establecen los parámetros de control de cerradura y equipo relacionado.

Toque **[Opciones de Acceso]** en la interfaz de Acceso.

Control de Acceso

Retardo de la cerradura: Tiempo en que la cerradura electrónica permanece abierta después de recibir la señal de abertura y hasta que se cierra automáticamente (el valor oscila entre 0 a 10 segundos).

Retardo de sensor de puerta: Cuando la puerta se abre, el sensor de la puerta se activará luego de un periodo de tiempo; si el Estado del Sensor de la puerta no coincide con el Tipo de Sensor de la Puerta, se activará una alarma. Este periodo de tiempo es el Retardo de Sensor de Puerta (el valor oscila entre 0 a 255 segundos).

Tipo de Sensor de la Puerta: Incluye Normalmente Abierto, Normalmente Cerrado y Ninguno. Ninguno significa que no está en uso el sensor de puerta; Normalmente Abierto significa que la puerta está abierta cuando tiene corriente eléctrica; Normalmente Cerrado significa que la puerta está cerrada cuando tiene corriente eléctrica.

Retardo de Alarma: Cuando el Estado del Sensor de la puerta no coincide con el Tipo de Sensor de la Puerta, se activará una alarma después de un periodo de tiempo; este periodo de tiempo es el Retardo de Alarma (el valor oscila entre 1 a 999 segundos)

Reintentos para Alarma: Cuando el número de verificaciones fallidas llega a un nivel establecido (de 1 a 9 veces), se activará la alarma. Si no se establece un valor, la alarma no se activará después de una verificación fallida.

Periodo de Tiempo NC: Establece el periodo de tiempo para el modo Normalmente Cerrado, de forma que nadie pueda tener acceso durante este periodo.

Periodo de Tiempo NO: Establece el periodo de tiempo para el modo Normalmente Abierto, de forma que la puerta siempre este abierta durante este periodo.

Lector RS485:

Días Festivos Válidos: Establecer si los ajustes del Periodo de Tiempo NC o del Periodo de Tiempo NO son válidos en los periodos establecidos como días festivos. Elija [ON] para habilitar los periodos de tiempo NC y NO en días festivos.

Altavoz de Alarma: Cuando el altavoz de alarma está habilitado, el altavoz sonará una alarma cuando el dispositivo esté siendo desmantelado.

Reiniciar Ajustes de Acceso: Restaura los parámetros de control de acceso.

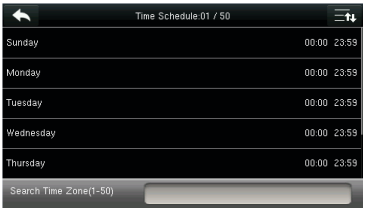
Nota: Después de establecer el Periodo de Tiempo NC, favor de cerrar bien la puerta, de lo contrario la alarma puede activarse durante el Periodo de Tiempo NC.

10.2 Ajustes de Horario

El horario es la unidad de tiempo mínima de los ajustes de control de acceso; se pueden establecer un máximo de 50 horarios en el sistema. Cada horario consiste de 7 secciones de tiempo (una semana) y cada sección de tiempo es el tiempo válido dentro de 24 horas.

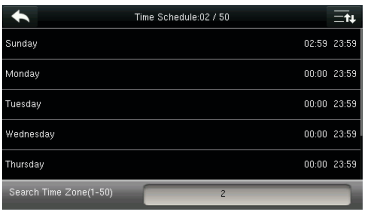
Control de Acceso

Toque **Horario** en la interfaz de **Acceso.**

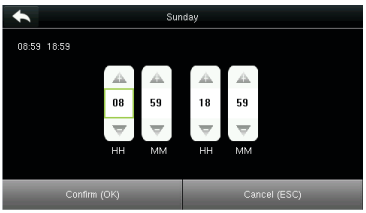


Toque la casilla de entrada de Buscar Horario

Introduzca el número de horario (Se pueden buscar hasta 50)



Toque la fecha en donde se requiera el ajuste de Horario.



Presione Arriba y Abajo para establecer la hora de Inicio y de Fin y después presione Confirmar (OK)

Horario Válido: 00:00 – 23:59 (Válido todo el día) o cuando la hora final sea mayor que la hora de inicio.

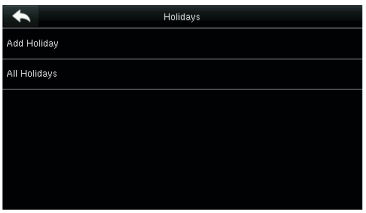
1. Horario Inválido: Cuando la hora final sea menor que la hora de inicio.
2. El horario predeterminado 1 indica que el sistema está abierto todo el día.

10.3 Ajustes de Días Festivos

En los días festivos y festivales se puede requerir de un control de acceso especial, pero cambiar el horario de acceso de todo el personal puede resultar tedioso; es por eso que ahora es posible configurar un horario de control de acceso para días festivos y festivales que aplique para todo el personal.

Control de Acceso

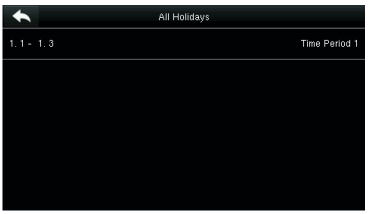
Toque **Días Festivos** en la interfaz de Acceso.



10.3.1 Agregar nuevo Día Festivo

Toque **Agregar Día Festivo** en la interfaz de Días Festivos.

Establecer parámetros de Día Festivo



Los Días Festivas se muestran en una lista

10.3.2 Editar Día Festivo

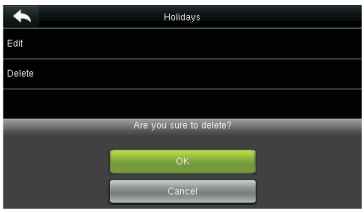
En la interfaz de Días Festivos, toque el día festivo que desee modificar.

Toque Editar

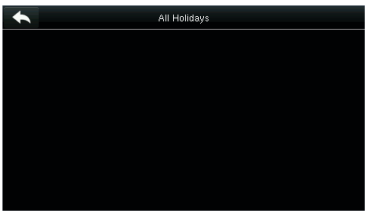
Modifique los parámetros de Día Festivo.

10.3.3 Borrar un Día Festivo

En la interfaz de Días Festivos, toque el día festivo que desee eliminar y toque Borrar.



Toque OK para confirmar la eliminación



Después de borrarlo, el día festivo ya no aparece en la lista

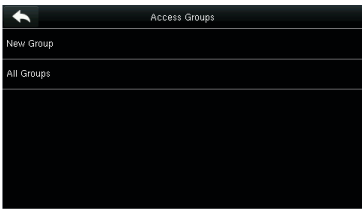
10.4 Ajustes de Grupos de Acceso

Agrupar es manejar usuarios en grupos.

El horario por defecto de los grupos de usuarios se establece como el horario grupal, mientras que los usuarios pueden establecer su horario personal. Cuando el modo de verificación de un grupo traslapa el modo de verificación de un usuario, el modo de verificación de usuario tiene prioridad.

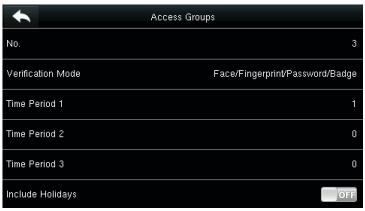
Cada grupo puede establecer cuando mucho 3 horarios, mientras al menos un horario sea válido, el grupo puede verificar exitosamente. Por defecto, los usuarios recién registrados pertenecen al grupo de Acceso 1 y pueden ser asignados a otro grupo de acceso.

Toca Grupos de Acceso en la interfaz de Acceso.

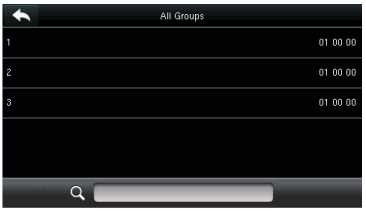


10.4.1 Agregar nuevo Grupo

Toque **Nuevo Grupo** en la interfaz de Acceso de Grupos.



Establezca los parámetros del Grupo de Acceso



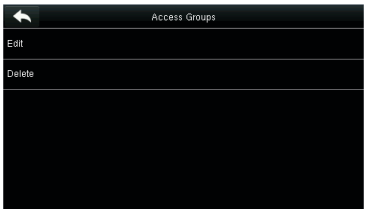
Los Grupos de Acceso agregados se muestran en una lista. Puedes buscar un grupo rápidamente por su número

Notas:

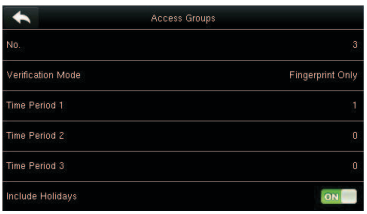
1. El sistema tiene un grupo de Acceso predeterminado con el número 1, que no puede eliminado, pero sí modificado.
2. Un número no puede ser modificado de nuevo después de establecerlo.
3. Cuando un día festivo se establece como válido, el personal en un grupo puede abrir la puerta sólo cuando el horario del grupo se traslapa con el horario del día festivo.
4. Cuando un día festivo se establece como inválido, el horario de control de acceso del personal en este grupo no se ve afectado por el día festivo.

10.4.2 Editar Grupo

En la interfaz Todos los Grupos seleccione el grupo que desee modificar.



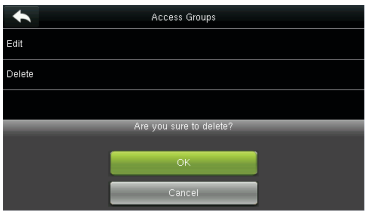
Toque Editar



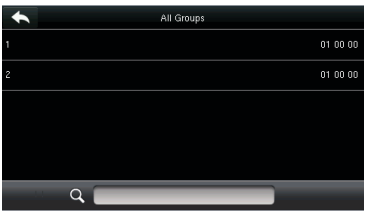
Modifique los parámetros de acceso de grupo.

10.4.3 Eliminar grupo.

En la interfaz Todos los Grupos seleccione el grupo que desee eliminar y toque Eliminar.



Toque OK para confirmar la eliminación



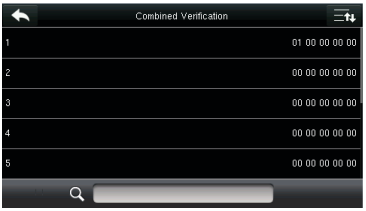
El Grupo de Acceso Eliminado ya no se muestra en Todos los Grupos

10.5 Configuración de Multi-Verificación

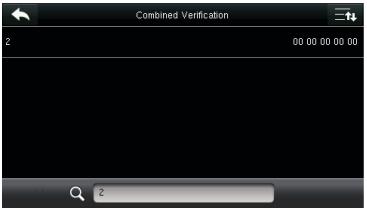
Combina 2 o más usuarios para activar la **Multi-Verificación** y así mejorar la seguridad.

Control de Acceso

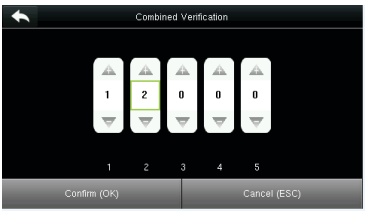
Toque **Multi-Verificación** en la interfaz de Acceso.



Toque la combinación de desbloqueo que desee configurar o toque la barra de búsqueda e introduzca el número de combinación de desbloqueo para encontrar una combinación especifica.



Toque una combinación de desbloqueo



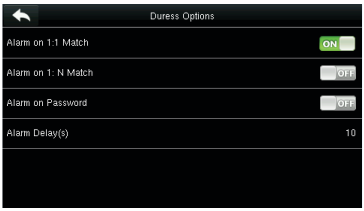
Toque arriba y abajo para introducir un numero de verificación y después toque Confirmar (OK).

Nota: En la multi-verifiación, el rango de números que pueden introducir los usuarios es de 0 a 5. Si necesita eliminar una combinación de desbloqueo, establece directamente todos los números de la combinación a 0. SI necesita modificar una combinación, toque directamente la combinación correspondiente para configurarlo de nuevo.

10.6 Configuración de Huella de Amago

Cuando el usuario se vea en una situación de amago o amenaza, seleccione el Modo de alarma de amago, la puerta se abrirá normalmente y se enviara una señal de alarma a la alarma discreta.

Toque **Opciones de Amago** en la interfaz Acceso.



Alarma en modo 1:1:Si está activada, cuando un usuario use el método de verificación 1:1 para verificar cualquier huella digital registrada, la alarma se activará. Si está desactivada, no se enviará la señal de alarma.

Alarma en modo 1: N: Si está activada, cuando un usuario use el método de verificación 1:N para verificar cualquier huella digital registrada, la alarma se activará. Si está desactivada, no se enviará la señal de alarma.

Alarma con Contraseña: Si está activada, cuando un usuario use el método de verificación con contraseña, la alarma se activará. Si está desactivada, no se enviará la señal de alarma.

Retardo de Alarma: Cuando se activa la alarma de amago, el dispositivo enviará la señal de alarma después de 10 segundos (predeterminado). Este valor puede cambiarse (el valor oscila de 1 a 999 segundos).

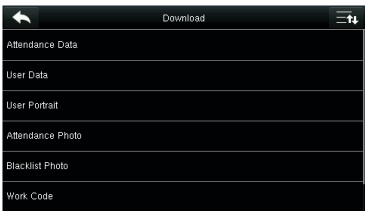
Gestión USB

Usted puede importar información de usuarios, plantillas de huellas digitales y datos de asistencia desde el dispositivo a un software de asistencia para su procesamiento o a otro dispositivo de huellas digitales por medio de una unidad USB. Antes de cargar/descargar datos desde/en una unidad USB, inserte la unidad en el puerto USB del dispositivo.

Toque **Gestión USB** en la interfaz del menú principal.

11.1 Descargar Datos

En la interfaz de **Gestión USB**, toque Descargar.



Datos de Asistencia: Descargar datos de asistencia de un periodo de tiempo específico en la unidad USB.

Datos de Usuario: Descargar toda la información de usuario y huellas digitales del dispositivo en la unidad USB.

Fotos de Usuario: Descargar todas las fotos de usuario del dispositivo en la unidad USB.

Fotos de Asistencia: Descargar todas las fotos de asistencia del dispositivo en la unidad USB.

Fotos de Lista Negra: Descargar todas las fotos de lista negra (fotos tomadas durante las verificaciones fallidas) del dispositivo en la unidad USB.

Código de Trabajo. - Guardar los códigos de trabajo del dispositivo en la unidad USB.

Mensaje Corto: Descargar los mensajes escritos en el dispositivo en la unidad USB.

11.2 Cargar Datos

En la interfaz de **Gestión USB**, toque **Cargar.**

Datos de Usuario: Cargar toda la información de usuario y huellas digitales desde la unidad USB al dispositivo.

Foto de Usuario: Para cargar una foto en formato JPG de la unidad USB al dispositivo. Durante la carga, puede seleccionar Cargar Foto Seleccionada o Cargar Todas las Fotos. La foto se muestra después de una verificación exitosa.

Durante la carga, se necesita crear una carpeta llamada "picture" en la carpeta raíz de la unidad USB y poner las fotos de usuarios dentro de ella. El sistema soporta un máximo de 2000 fotos y cada una no puede excederse de 20 KB. Las fotos deben nombrarse en el formato X.jpg, donde X indica el número de ID del usuario.

Gestión USB

Código de Trabajo: Para cargar códigos de trabajo desde la unidad USB al dispositivo.

Mensaje Corto: Para cargar mensajes cortos guardados en la unidad USB al dispositivo.

Protector de Pantalla: Para cargar protectores de pantalla de la unidad USB al dispositivo. Durante la carga, puede seleccionar Cargar Foto Seleccionada o Cargar Todas las Fotos. Las imágenes se mostrarán en la interfaz de espera del dispositivo después de la carga. Durante la carga, se necesita crear una carpeta llamada "**advertise**" en la carpeta raíz de la unidad USB y poner las imágenes a usar como protectores dentro de ella. El sistema soporta un máximo de 20 fotos y cada una no puede excederse de 30 KB. El nombre y formato de las imágenes no está limitado, soportando formatos como jpg, png y bmp.

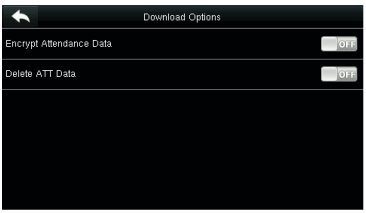
Fondo de Pantalla: Para cargar fondos de pantalla de la unidad USB al dispositivo. Durante la carga, puede seleccionar Cargar Foto Seleccionada o Cargar Todas las Fotos. Las imágenes se mostrarán en la pantalla principal después de la carga.Durante la carga, se necesita crear una carpeta llamada "**wallpaper**" en la carpeta raíz de la unidad USB y poner las imágenes a usar como fondo dentro de ella. El sistema soporta un máximo de 20 fotos y cada una no puede excederse de 30 KB. El nombre y formato de las imágenes no está limitado, soportando formatos como jpg, png y bmp.

Nota: El tamaño de una sola foto de usuario o foto de asistencia no puede exceder 10KB y el dispositivo puede almacenar un total de 10,000 fotos de usuario o de asistencia.

El tamaño óptimo para una imagen de fondo o protector de pantalla es de 640*480.

11.3 Opciones de Descarga

En la interfaz de **Gestión USB**, toque **Opciones de Descarga**.



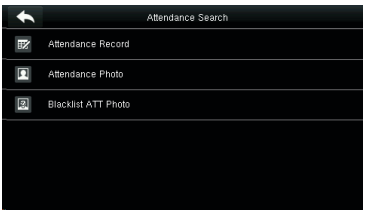
Encriptar datos de asistencia: Durante la carga y descarga, los datos de asistencia están encriptados.

Borrar Eventos Después de Descargar: Después de descargar los datos de asistencia exitosamente a la unidad USB, los datos en el dispositivo son eliminados.

Buscar Registros de Asistencia

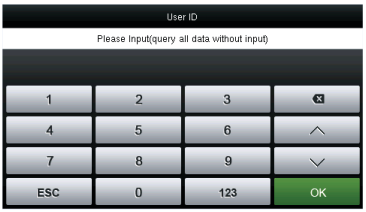
Cuando los usuarios se verifican de forma exitosa, se guardan registros de asistencia en el dispositivo. Esta función permite a los usuarios ver registros de asistencia.

Toque **Eventos** en el menú principal.

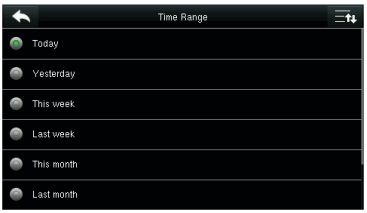


El proceso de búsqueda de fotos de asistencia y fotos de lista negra es el mismo que el de la búsqueda de registros de asistencia. A continuación, se muestra un ejemplo de búsqueda de registros de asistencia.

En la interfaz **Eventos**, toque **Registros de Asistencia.**

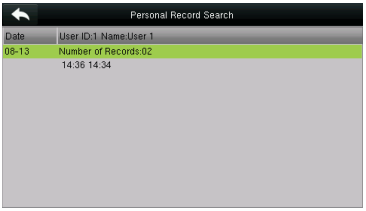


Introduzca el ID del usuario que desee buscar y toque **OK**. Tocar **OK** sin introducir un ID de usuario realiza la búsqueda de registros de asistencia de todos los empleados.

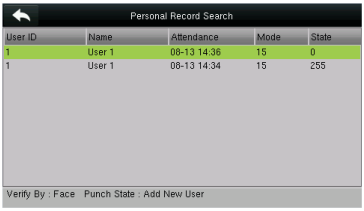


Seleccione el rango de tiempo para la búsqueda de registros de asistencia.

Buscar Registros de Asistencia



La búsqueda se realiza con éxito. Toque un registro en color verde para ver sus detalles.

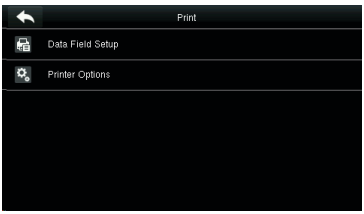


La imagen muestra los detalles para este registro.

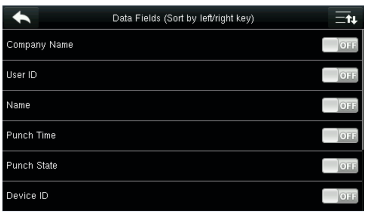
Ajustes de Impresión

Los dispositivos con la función de Impresión pueden imprimir registros de asistencia cuando se les conecta una impresora (esta función es opcional y solo puede ser agregada en algunos productos).

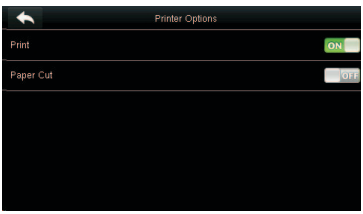
Toque **Imprimir** en la interfaz del menú principal.



Toque **Configurar Campos** en la interfaz Imprimir.



Presione **ON/OFF** para activar o desactivar los campos de datos que necesita imprimir.



Presione **ON/OFF** para activar o desactivar la función de **Corte de Papel.**

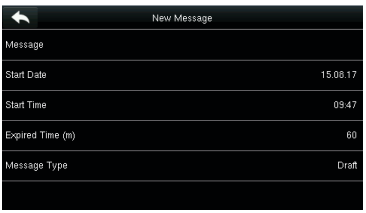
Nota: Para activar la función de Corte de Papel, se necesita conectar al dispositivo una impresora con la función de corte de papel, de forma que la impresora corte los papeles de acuerdo a la información de impresión seleccionada en el dispositivo.

Mensaje Corto

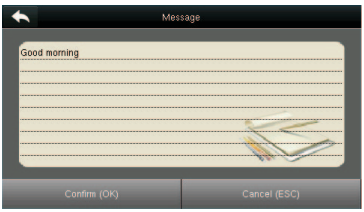
El operador puede crear notificaciones de antemano y plasmarlos en forma de mensajes cortos o SMS que se muestran en la pantalla. Los mensajes pueden ser públicos o personales. Si se crea un mensaje público, se mostrará el ícono en la columna de información que está en la parte superior de la interfaz de espera durante un tiempo determinado. Si se crea un mensaje personal, el empleado receptor del mensaje puede leerlo después de una verificación exitosa.

14.1 Agregar un Nuevo Mensaje Corto

1. Escribir el contenido del mensaje:

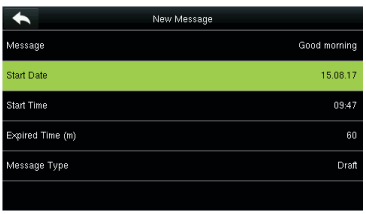


Toque **Mensaje**

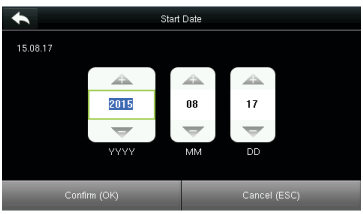


Escriba el contenido del mensaje y toque OK para guardar y salir

2. Establecer la hora y fecha inicial del mensaje:



Seleccione **Fecha Inicial** y toque **OK**



Presione las teclas numéricas en el teclado para establecer la fecha y presione **OK.**

Mensaje Corto

3. Establecer Tiempo de Expiración (m): Los mensajes se muestran durante un tiempo efectivo. Después de ese tiempo, dejan de mostrarse.

Nota: Para mensajes públicos, el tiempo efectivo también es el tiempo de visualización. Para los mensajes personales, se necesita establecer un tiempo de visualización después del tiempo efectivo. Es decir, el tiempo de visualización de un mensaje personal se muestra cuando se registra una entrada o salida durante el tiempo efectivo del mensaje.

4. Establecer Tipo de Mensaje

Público: El mensaje puede verse por todos los empleados.

Personal: El mensaje está dirigido a un solo empleado.

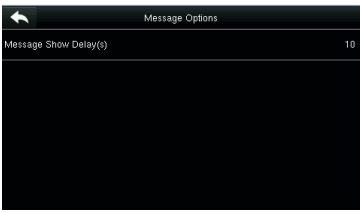
Borrador: Un mensaje predeterminado. No hay diferencia con el mensaje público o personal.

Seleccione **Tipo de Mensaje** y toque **OK.**

Presione ▼ para seleccionar un tipo y toque **OK** para confirmar.

14.2 Opciones de Mensaje

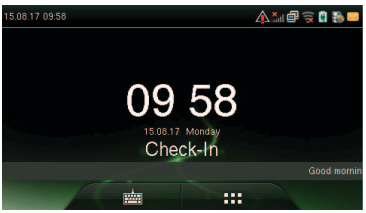
Seleccione el tiempo de visualización de un mensaje personal en la interfaz inicial.



14.3 Ver Mensajes Públicos y Mensajes Personales.

Después de que se establezca un mensaje público, el ícono de mensaje se muestra en la parte superior derecha la interfaz principal. El contenido del mensaje público se muestra desplazándose en la pantalla.

El contenido de un mensaje personal se muestra se muestra después de una verificación exitosa del usuario.

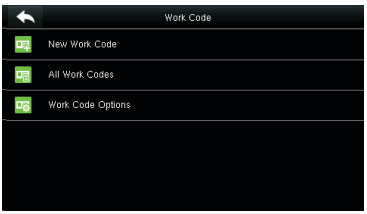


El mensaje público se muestra desplazándose en la parte inferior de la interfaz.

El mensaje privado se muestra después de una verificación exitosa.

Código de Trabajo

El salario que perciben los empleados está sujeto a sus registros de asistencia. Algunos empleados pueden realizar diferentes tipos de trabajo que pueden manejar diferentes periodos de tiempo. Considerando que el salario puede variar según los tipos de trabajo, la terminal proporciona un parámetro para indicar el correspondiente tipo de trabajo para cada registro de asistencia y así facilitar en entendimiento de las diferentes situaciones de asistencia durante el manejo de los datos de asistencia.

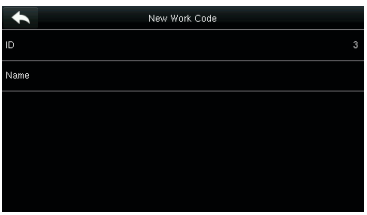


15.1 Agregar Código de Trabajo

ID: Un código digital para distinguir el código de trabajo.

Nombre: El nombre o significado del código de trabajo.

1. Editar un ID

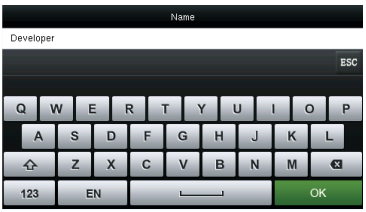


Toque ID

Presione el teclado numérico para asignar un número entre 1-99999999.

2. Editar un Nombre

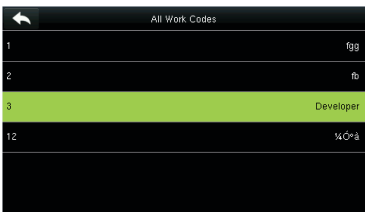
Toque **Nombre**



Presione * para elegir un teclado y escriba un nombre.

15.2 Ver Todos los Códigos de Trabajo

Usted puede ver, editar y eliminar códigos de trabajo en la interfaz Todos los Códigos de Trabajo. El proceso de editar un código de trabajo es el mismo que el de agregar un código de trabajo con la diferencia de que el ID no se puede modificar.



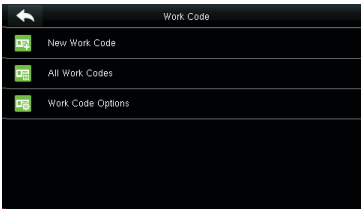
Ver la información de todos los códigos de trabajo.

Editar o eliminar un código de trabajo.

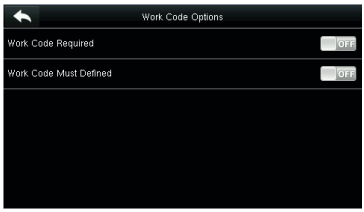
Código de Trabajo

15.3 Opciones del código de trabajo.

Esta sección sirve para especificar si el código de trabajo debe introducirse y si el código de trabajo introducido debe existir durante la verificación.



Selecciona **Opciones de Código de Trabajo.**

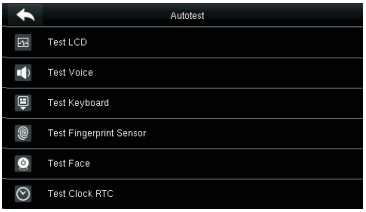


Presiona **ON/OFF** para activar o desactivar las opciones.

Test Automático

El test automático permite al dispositivo comprobar el funcionamiento correcto de varios módulos, incluyendo la pantalla LCD, sonido, sensor de huellas, teclado táctil, cámara y reloj.

En la pantalla inicial, presione **Pruebas** para entrar a la interfaz de Pruebas.



Probar LCD: Probar los efectos de color de la pantalla LCD mostrando imágenes en colores vivos, blanco y negro para comprobar si la pantalla está funcionando adecuadamente.

Probar Sonido: La terminal probará automáticamente si los archivos de voz están completos y que la calidad del sonido sea la adecuada reproduciendo los archivos de sonido almacenados dentro de la misma.

Probar Sensor de Huellas: Probar si el sensor de huellas digitales encuentra funcionando con normalidad y si la calidad de las imágenes de las huellas es apta. Cuando el usuario presione el dedo en el sensor, la imagen de la huella será mostrada en tiempo real.

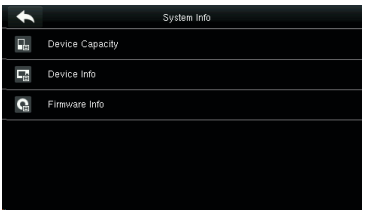
Probar Rostro: Probar si la cámara funciona adecuadamente verificando que las fotos capturadas sean claras.

Probar Reloj RTC: Probar el Reloj en Tiempo Real. La terminal revisará el rendimiento del reloj examinando el cronómetro del reloj. Presione la pantalla para iniciar el conteo y presiónela de nuevo para detenerlo.

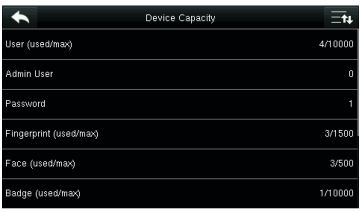
Información del Sistema

Con este parámetro usted puede verificar el estado de almacenamiento, información del dispositivo y la información del firmware.

Toque **Información** en la interfaz del menú principal.



En la interfaz de información, toque el apartado que desea explorar



Toque Capacidad del Equipo para ver la información sobre el almacenamiento de datos del dispositivo.

Toque Información del Equipo para ver información sobre el dispositivo.

Toque **Información de Firmware** para ver información del firmware instalado en el dispositivo.

Anexo

Anexo 1: Introducción a Wiegand

El protocolo Wiegand26 es un protocolo estándar de control de acceso desarrollado por el Subcomité de Estándar de Control de Acceso afiliado a la Asociación de la Seguridad Industrial (SIA por sus siglas en inglés). Es un protocolo usado para puertos y salidas de lectores de tarjetas IC sin contacto.

El protocolo define la conexión entre el lector de tarjetas y el controlador los cuales son ampliamente usados en la industria del control de acceso, seguridad, entre otras. Esto ha estandarizado el trabajo de los diseñadores de lectores de tarjetas y fabricantes de controladores. Los dispositivos de control de acceso producidos por nuestra empresa también aplican este protocolo.

Señal Digital

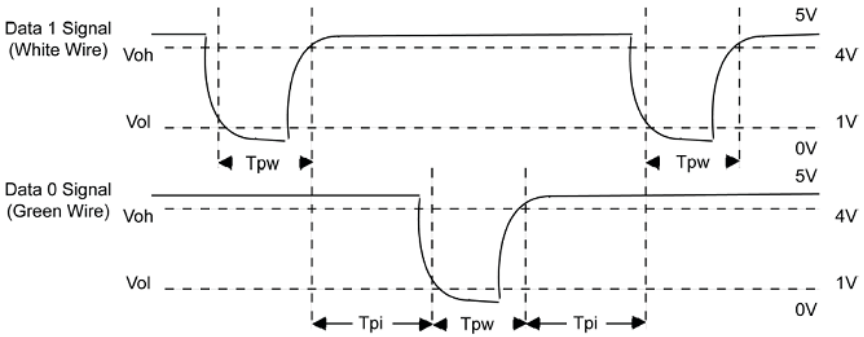
La figura 1 muestra el diagrama secuencial del lector de tarjetas que envía señales digitales en bits hacia el controlador de acceso.

El Wiegand en este diagrama sigue el protocolo estándar de control de acceso de la SIA, que tiene como objetivo lectores de tarjetas Wiegand de 26 bits (con un tiempo de pulso de entre 20us hasta 100us y un tiempo de salto de pulso de entre 200us hasta 20ms). Las señales Data0 y Data1 son de alto nivel (más que Voh) hasta que el lector de tarjetas está listo para enviar un flujo de datos. El lector de tarjetas envía un pulso asíncrono de bajo nivel (menor que vol), transmitiendo un flujo de datos a través de los cables Data1 y Data0 para acceder a la caja de control (como se ve en el diente de sierra de la figura 1). Los pulsos Data0 y Data1 no se traslapan ni sincronizan. La figura 1 muestra la máxima y mínima amplitud de pulso (pulsos sucesivos) y el tiempo de salto de pulso (el tiempo entre 2 pulsos) permitido por las terminales de control de acceso de huellas digitales de la serie F.

Tabla 1: Tiempo de Pulso

Señal	Definición	Valor Típico del Lector de Tarjeta
Tpw	Amplitud de Pulso	100 µs
Tpi	Intervalo de Pulso	1 ms

Figura 1: Diagrama Secuencial



Los formatos Wiegand de 26 bits y de 34 bits se describen a continuación:

• Wiegand 26

El sistema tiene integrado un formato Wiegand de 26 bits. Presione Formato Wiegand y seleccione "Estándar Wiegand 26-bits".

La composición del formato Wiegand de 26 bits contiene 2 bits de paridad y 24 bits para contenido de salida ("ID de Usuario" o "Número de Tarjeta"). El código binario de 24 bits representa hasta 16,777,126 (0 - 16,777,215) valores diferentes.

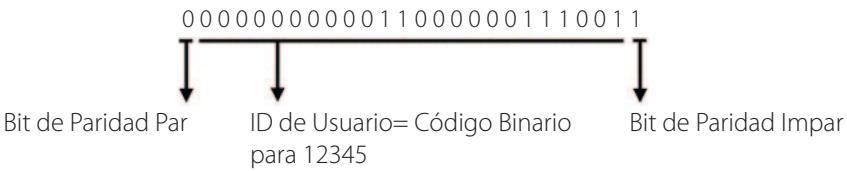
1	2 25	26
Bit de Paridad Par	ID de Usuario/ Número de Tarjeta	Bit de Paridad Impar

Definición de los campos:

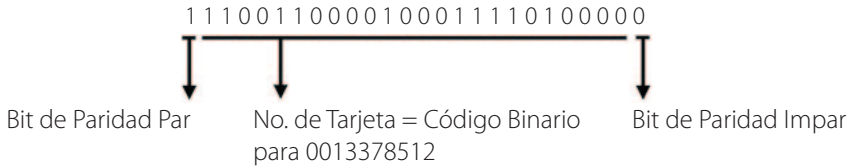
Campo	Significado
Bit de paridad par	Evaluado desde el bit 2 al bit 13. El bit de paridad par es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad par es 0.
ID de Usuario/Número de Tarjeta (bit 2 – bit 25)	ID de Usuario/Número de Tarjeta (Código de Tarjeta, 0 – 16777215). El bit 2 es el Bit Más Importante (MSB por siglas en inglés)
Bit de paridad impar	Evaluado desde el bit 14 al bit 25. El bit de paridad impar es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad impar es 0.

Por ejemplo, para un usuario con ID de usuario 12345, con número de tarjeta 0013378512 y el número de ID fallida se estableció en 1.

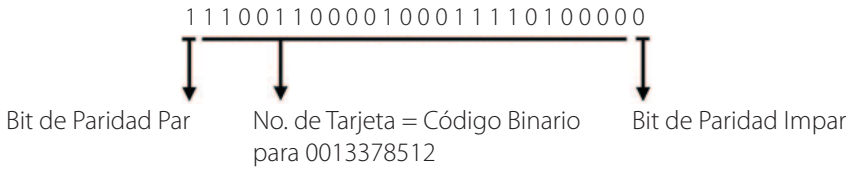
1. Cuando la salida se establece como "ID de Usuario", la salida Wiegand es la siguiente después de la verificación exitosa:



2. Cuando la salida se establece como "Número de Tarjeta", la salida Wiegand es la siguiente después de la verificación exitosa:



3. Cuando la verificación falla, la salida wiegand es la siguiente.



Nota: Si el contenido de salida excede el alcance de todos los valores permitidos por el formato Wiegand, los últimos bits se tomarán y los primeros bits se descartarán automáticamente. Por ejemplo, el ID de Usuario 888 888 888 es 110 100 111 110 110 101 111 000 111 000 en formato binario. Wiegand 26 sólo soporta 24 bits, eso es, sólo toma en cuenta los últimos 24 bits, mientras que los primeros 6 bits "110 100" son automáticamente descartados.

• Wiegand 34

El sistema tiene integrado un formato Wiegand de 34 bits. Presione Formato Wiegand y seleccione "Estándar Wiegand 34-bits".

La composición del formato Wiegand de 34 bits contiene 2 bits de paridad y 32 bits para contenido de salida ("ID de Usuario" o "Número de Tarjeta"). El código binario de 32 bits representa hasta 4,292,967,296 (0 - 4,292,967,296) valores diferentes.

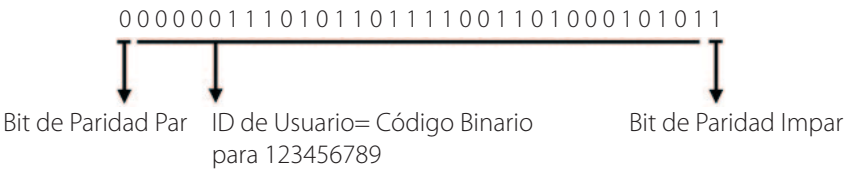
1	2 33	34
Bit de Paridad Par	ID de Usuario/ Número de Tarjeta	Bit de Paridad Impar

Definición de los campos:

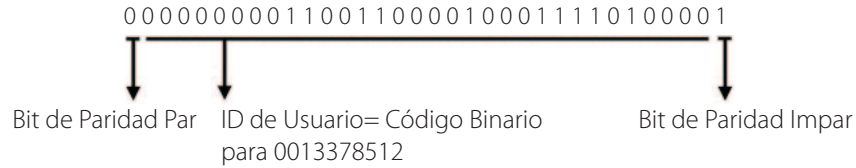
Campo	Significado
Bit de paridad par	Evaluado desde el bit 2 al bit 17. El bit de paridad par es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad par es 0.
ID de Usuario/Número de Tarjeta (bit 2 – bit 25)	ID de Usuario/Número de Tarjeta (Código de Tarjeta, 0 – 16777215). El bit 2 es el Bit Más Importante (MSB por siglas en inglés)
Bit de paridad impar	Evaluado desde el bit 18 al bit 33. El bit de paridad impar es 1 si el carácter tiene un número par de 1 bit; de lo contrario, el bit de paridad impar es 0.

Por ejemplo, para un usuario con ID de usuario 123456789, con número de tarjeta 0013378512 y el número de ID fallida se estableció en 1.

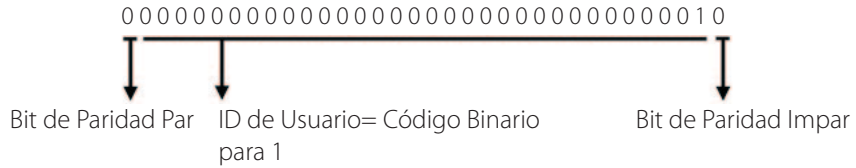
1. Cuando la salida se establece como "ID de Usuario", la salida Wiegand es la siguiente después de la verificación exitosa:



2. Cuando la salida se establece como "Número de Tarjeta", la salida Wiegand es la siguiente después de la verificación exitosa:



3. Cuando la verificación falla, la salida Wiegand es la siguiente.



Anexo 2: Funciones de Impresión

Nota: Sólo algunos modelos soportan la función de impresión.

Instrucciones de Función

Esta función sólo soporta el puerto de comunicación serial, pero no soporta impresión por puertos paralelos. El contenido a imprimir es enviado a través del formato RS232; cada vez se enviará información de verificación al puerto serial. La impresión está disponible si se conecta una impresora, pero también puede usarse una hyper terminal para leer el contenido de salida.

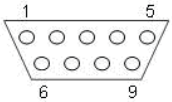
Conexión entre el dispositivo y la impresora.	Dispositivo Impresora 2 TXD ⟷ 3 RXD 3 RXD ⟷ 2 TXD 5 GND ⟷ 7FG
Orden de pines de RS232	

Diagrama de Conexión

Operación

1. En la interfaz principal, presione (M/OK) > Comunicación > Comunicación Serial > Velocidad de Baudios y elija 19200.

2. En la interfaz inicial, presione (M/OK) > Imprimir para establecer el formato y parámetros de impresión. Favor de consultar 13 Ajustes de Impresión *

Nota:

1.- La velocidad de baudios del dispositivo e impresora (hyper terminal) debe ser consistente.

2.- Si el formato de impresión predeterminado no es satisfactorio, usted puede contactar a nuestra empresa para configurar otros formatos.

Anexo 3: Declaración de Derechos Humanos y de Privacidad.

Apreciado consumidor:

Gracias por elegir los productos biométricos híbridos diseñados y fabricados por el equipo ZK. Como proveedor líder en el mercado de productos y soluciones biométricas, nos esforzamos por cumplir los estatutos relacionados con los derechos humanos y privacidad de cada país al mismo tiempo que continuamos con la investigación y desarrollo de nuevos productos.

Por esta razón consignamos en este documento la siguiente información:

1. Todos dispositivos de reconocimiento de huella digital ZKTeco para uso civil, sólo recogen puntos característicos de las huellas digitales, no imágenes como tal. Gracias a esto no se suscitan problemáticas que involucren o vio¬len la privacidad de los usuarios.

2. Los puntos característicos de las huellas digitales recolectadas por nuestros dispositivos no pueden ser utilizadas para reconstruir la imagen original de la huella.

3. ZKTeco, como proveedor de los equipos, no se hace legalmente responsable, directa o indirectamente, por ninguna consecuencia generada debido al uso de nuestros productos.

4. Para cualquier inconveniente que involucre derechos humanos o privacidad al usar nuestros productos, por favor contacte directamente a su empleador.

Anexo

Nuestros otros equipos de huella digital de uso policíaco u herramientas de desarrollo, pueden proporcionar la función de recolección de las imágenes originales de las huellas digitales. Cuando considere que este tipo de recolección de huellas infringe su privacidad, por favor contacte al gobierno local o al proveedor final. ZKTeco, como el fabricante original de los equipos, no se hace legalmente responsable de ninguna infracción generada por esta razón.

Nota: Las siguientes son regulaciones ligadas a las leyes de la República popular de China acerca de la libertad personal:

1. Detención, reclusión o búsqueda ilegal de ciudadanos de la República Popu¬lar de China es una violación a la intimidad de la persona, y está prohibida.

2. La dignidad personal de los ciudadanos de la República Popular de China es inviolable.

3. El hogar de los ciudadanos de la República Popular de China es inviolable.

4. La libertad y privacidad correspondiente a los ciudadanos de la República Popular de China están protegidos por la ley.

Recalcamos que la biometría, como avanzada tecnología de reconocimiento, será aplicada en diversos sectores; incluyendo el comercio electrónico, sistemas bancarios, aseguradoras y cuestiones legales. Cada año alrededor del mundo, una gran cantidad de personas sufren inconvenientes causados por la inseguridad de las contraseñas.

En la actualidad, el reconocimiento de huellas digitales es utilizado para una protección adecuada de la identidad de las personas brindando un ambiente de alta seguridad en todo tipo de empresa.

Anexo 4. Uso amigable con el Medio Ambiente

Descripción de Uso Amigable con el Medio Ambiente.

- El EFUP (Periodo de Uso Amigable con Medio Ambiente, por sus siglas en inglés) marcado en este producto se refiere al periodo de seguridad en el cual el producto es utilizado bajo las condiciones establecidas en las instrucciones del mismo, sin riesgo de fuga de sustancias nocivas o perjudiciales.

- El EFUP de este producto no cubre las partes consumibles que necesiten ser reemplazadas regularmente, por ejemplo, baterías. El EFUP de las baterías es de 5 años.

Nombre y concentración de sustancias o elementos nocivos						
Nombre de las piezas	Sustancias o elementos nocivos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Resistencia	X	O	O	O	O	O
Condensador	X	O	O	O	O	O
Inductor	X	O	O	O	O	O
Diodo	X	O	O	O	O	O
Componentes ESD	X	O	O	O	O	O
Buzzer	X	O	O	O	O	O
Adaptador	X	O	O	O	O	O
Tornillos	O	O	O	X	O	O

O: Indica que esta sustancia tóxica o nociva está presente en todos los materiales homogéneos de esta pieza, por debajo de los límites requeridos en SJ/T11363-2006.

X: Indica que esta sustancia tóxica o nociva está presente en al menos uno de los materiales homogéneos de esta pieza, por encima de los límites requeridos en SJ/T11363-2006.

Nota: El 80% de las partes de este producto están fabricadas con materiales ecológicos. Las sustancias o elementos nocivos contenidos, no pueden ser reemplazados por materiales ecológicos por razones técnicas o restricciones económicas.

Green Label

German Centre 3-2-02, Av. Santa Fe No. 170, Lomas de Santa Fe,
Delegación Alvaro Obregón, 01210 México D.F.
Tel: +52 (55) 52-92-84-18
www.zktecolatinoamerica.com
www.zkteco.com