MANUAL DE USUARIO

ProCapture-X
Dispositivos de Control de Acceso

Versión: 1.0
Noviembre 2016

Acerca de este manual

Este manual presenta el funcionamiento de las interfaces de usuario y funciones del menú de la terminal de control de acceso con pantalla TFT de 2.4 pulgadas y POE ProCapture-X.

Las imágenes usadas en este manual pueden no ser completamente consistentes con las del producto adquirido. Prevalecerán las imágenes del producto real.

Las funciones marcadas con * no están disponibles en todos los dispositivos.

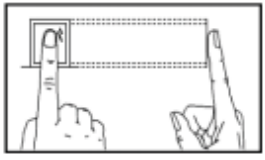
Contenido

Notas de Orientación

1.1 Método para colocar la huella digital

Es recomendable utilizar el dedo índice, dedo medio, o dedo anular, evitar el uso del dedo pulgar o del meñique.

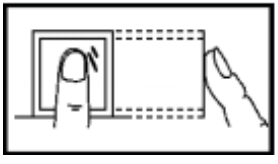
1. Forma correcta de colocar la huella digital:



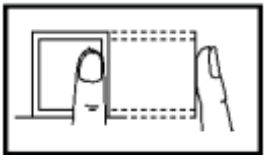
Presione el dedo horizontalmente en el sensor de huellas digitales; el centro de la huella digital se debe colocar en el centro del sensor.

2. Formas incorrectas de colocar la huella digital:

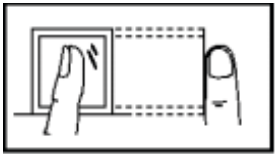
Vertical



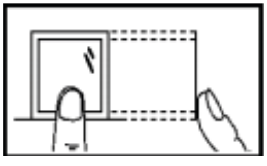
A los lados



Inclinado



Demasiado abajo



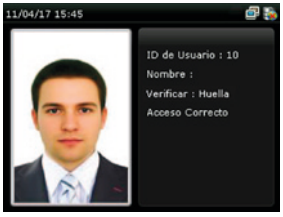
Utilice el método correcto para colocar las huellas digitales para el registro y la verificación. Nuestra empresa no asume la responsabilidad por el mal desempeño de la verificación causado por la operación incorrecta del usuario. Los derechos a la interpretación final y modificación están reservados.

1.2 Métodos de Verificación

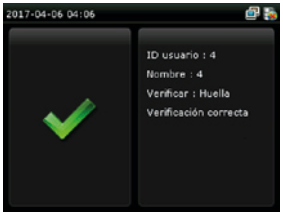
1.2.1 Verificación de Huellas Digitales 1:N

En el método de verificación de huellas digitales 1:N, una huella digital es obtenida por el sensor y se verifica con todas las huellas digitales almacenadas en el dispositivo.

Utilice la forma correcta de colocar la huella digital en el sensor (para obtener instrucciones detalladas, consulte 1.1 Método para colocar la huella digital)



Verificación exitosa



Verificación exitosa

Verificación fallida

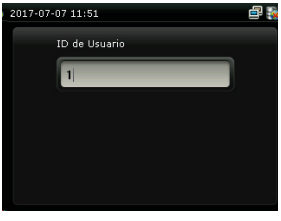
Observaciones:

En los dispositivos que posean la función ID con Foto, se mostrará la figura 1 en la pantalla después una verificación exitosa, de lo contrario, se mostrará la figura 2 después de una verificación exitosa.

*** Sólo algunos productos están equipados con la función ID con Foto.**

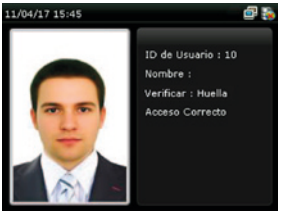
1.2.2 Verificación de Huellas Digitales 1:1

En el método de verificación de huellas digitales 1:1, la huella digital es obtenida por el sensor y se verifica con la huella digital correspondiente al ID de usuario introducido previamente. Favor de usar este método de verificación cuando sea difícil reconocer la huella en el método 1:N.

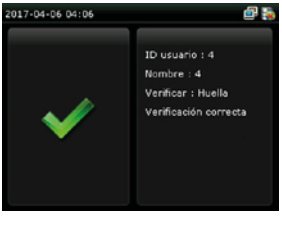


Introduzca el ID del usuario y presione

Presione ▼ para elegir "Huella" y pulse ⏎. Después coloque el dedo sobre el sensor.



Verificación Exitosa



Verificación Exitosa

Verificación Fallida

Observaciones:

1. Introduzca el ID de Usuario y presione ⏎. Si se muestra el mensaje "¡ID no válido!" esto significa que el ID de usuario no existe.

2. Cuando el dispositivo muestra "Intente de nuevo por favor", coloque de nuevo su dedo en el sensor de huellas digitales. Si la verificación falla aún después de 2 intentos, saldrá a la interfaz inicial.

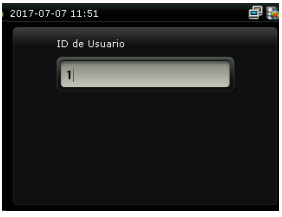
3. Los dispositivos que cuenten con la función ID con Foto mostrarán la figura 3 después de una verificación exitosa, de lo contrario, se mostrará la figura 4.

*** Sólo algunos productos están equipados con la función ID con Foto.**

Notas de Orientación

1.2.3 Verificación con Contraseña

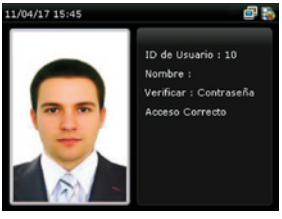
En este método de verificación, la contraseña introducida se verifica con la contraseña del ID de usuario.



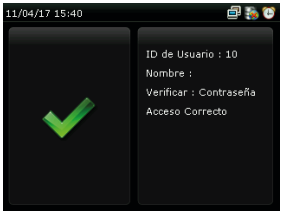
Introduzca el ID del usuario y presione

Seleccione "**Contraseña**" y presione

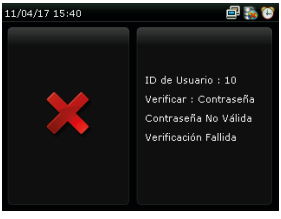
Introduzca la contraseña



Verificación Exitosa



Verificación Exitosa



Verificación Fallida

Observaciones:

1. Si se muestra el mensaje "Contraseña Incorrecta", por favor introduzca la contraseña de nuevo. Si la verificación falla aún después de 2 intentos, saldrá a la interfaz inicial.

2. En los dispositivos con la función ID con Foto, la figura 4 se mostrará en la pantalla después de una verificación exitosa, de no contar con la función, se mostrará la figura 5.

1.2.4 Verificación con Tarjeta

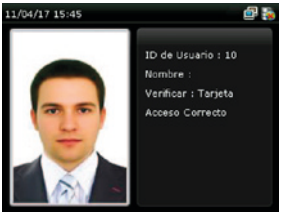
Observaciones:

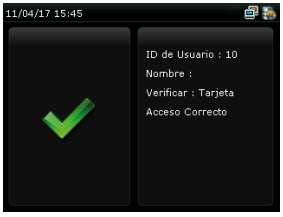
Sólo los productos con un módulo de tarjetas integrado están equipados con la función de verificación con tarjeta. Por favor, póngase en contacto con nuestro soporte técnico según sea necesario.

1. Deslice la tarjeta por encima del lector de tarjetas (la tarjeta ya debe estar registrada).

2. Verificación exitosa.

3. Verificación fallida.





En los dispositivos con la función ID con Foto, la figura 4 se mostrará en la pantalla después de una verificación exitosa, de no contar con la función, se mostrará la figura 5.

*** Sólo algunos productos están equipados con la función ID con Foto.**

Notas de Orientación

1.3 Interfaz Inicial

Cuando el dispositivo está encendido, la interfaz inicial se muestra como a continuación:

Menú Principal

Cuando el dispositivo está en modo de espera, presione [→] para entrar al menú principal.

Existen 11 opciones en el menú principal del dispositivo:

	Usuarios	Usted puede administrar la información de los usuarios registrados incluyendo ID de usuario, privilegios, huella digital, tarjeta (las tarjetas ID y MiFare son opcionales), contraseña y privilegios de control de acceso.
	Privilegios	Aquí puede asignar los privilegios de cada usuario de acceder a los menús y cambiar configuraciones.
	Red	Establecer los parámetros relacionados con la comunicación entre el dispositivo y la PC, incluyendo parámetros de Ethernet como la dirección IP, Conexión a PC, Red Inalámbrica* así como ajustes ADMS y Wiegand.
	Sistema	Para ajustar los parámetros relacionados del sistema y actualizar el firmware, incluyendo ajuste de fecha y hora, los registros de acceso, los parámetros de huellas digitales y restablecer la configuración de fábrica.
	Personalizar	Esto incluye la visualización de la interfaz, el sonido y la configuración del timbre.
	Datos	Borra los registros de acceso, borrar todos los datos, borrar privilegio de administrador, elimine los protectores de pantalla y copia de seguridad y restauración de datos.

Menú Principal

	Acceso	Para ajustar los parámetros de los dispositivos de control de cerradura y de acceso, incluidos los parámetros de control de acceso, horario, días de festivos, verificación multi-usuario y anti-passback.
	Gestión USB	Para transferir datos tales como datos de usuario y los registros de acceso desde la unidad USB al software de apoyo u otros dispositivos.
	Eventos	Para buscar los registros almacenados en el dispositivo después de la verificación exitosa.
	Pruebas	Para probar de forma automática funciones diferentes módulos, incluyendo la pantalla LCD, voz, teclado, sensor de huellas digitales, la cámara y el reloj de tiempo real.
	Información	Para comprobar la capacidad, información y firmware actual del dispositivo.

Fecha/Hora

En la interfaz inicial, pulse > **Sistema**> **Fecha y Hora** para entrar en la Interfaz de configuración de la fecha / hora. Se incluye el establecimiento de la fecha, hora, reloj de 24 horas, formato de fecha y el horario de verano.
Al restablecer la configuración de fábrica, el formato de fecha puede ser restaurado (AAAA-MM-DD).

Observaciones:

Al restablecer la configuración de fábrica, no se restaurará la fecha / hora del dispositivo (si la fecha / hora se ajusta a 18:30 el 1 de enero de 2020, después de reestablecer los ajustes, la fecha / hora se mantendrá en 18: 30 de 1 de enero, 2020.

3.1 Cambio de Horario

El Horario de Verano, también llamado DST, es un sistema de ajuste de la hora local con el fin de ahorrar energía.

El tiempo que se adopta durante las fechas establecidas se llama "Horario de Verano". Por lo general, se adelanta una hora en verano para aprovechar mejor la iluminación y ahorrar energía. En otoño, el tiempo se reanudará el tiempo estándar. Las regulaciones son diferentes en distintos países. En la actualidad, cerca de 110 países adoptan el horario de verano.

El dispositivo puede adoptar el cabio de horario adelantando una hora a las XX (hora) XX (día) XX (mes), y retrocediendo una hora a las XX (hora) XX (día) XX (mes). Por ejemplo, ajuste el reloj para que se adelante una hora a las 08:00 del 1 de Abril y que retroceda una hora a las 08:00 el 1 de Octubre.

Fecha/Hora

Presione > **Sistema**> **Fecha y Hora**> **Cambio de Horario,** a continuación, pulse > para activar el Horario de Verano.

Modo de Cambio de Horario: Elija el modo del cambio de horario. Puede elegir entre el modo por fecha/hora o el modo por semana/día.

Ajustes de Cambio de Horario: Ajuste la fecha/hora o la semana/día del cambio de horario de acuerdo al modo seleccionado.

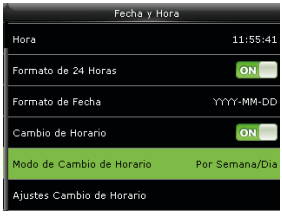
¿Cómo establecer el cambio de horario?

Por ejemplo, adelantar el reloj una hora a las 08:00 el 1 de abril y retrasar una hora a las 08: 00 el 1 de octubre (el sistema vuelve a la hora original).

Por el modo de fecha / hora:

Fecha/Hora

Por el modo de semana / día:



Observaciones:

1. Si el mes en que se inicia el cambio de horario es posterior al mes en que termina, el cambio de horario se extiende por dos años diferentes. Por ejemplo, la hora de inicio del cambio de horario es 2014-9-1 las 4:00 y la hora de finalización es 2015-4-1 a las 4:00.

2. Supongamos que el modo de semana/día fue seleccionado en **[Modo de Cambio de horario]** y el cambio de horario comienza desde el domingo de la sexta semana de septiembre de 2013. De acuerdo con el calendario, septiembre de 2013 no tiene seis semanas sino 5. En este caso, en 2013, el cambio de horario comienza en el punto de tiempo correspondiente del último domingo de septiembre.

3. Supongamos que el cambio de horario se inicia desde el lunes de la primera semana de septiembre de 2015. De acuerdo con el calendario, la primera semana de septiembre de 2015 no tiene lunes. En este caso, el cambio de horario se inicia desde el primer lunes de septiembre de 2015.

Usuarios

4.1 Agregar Usuario

Aquí puede registrar un usuario nuevo incluyendo a un administrador o a un usuario normal.

En la interfaz inicial, pulse > **Usuarios** > **Nuevo Usuario.**

Los ajustes incluyen establecer el ID de usuario, elegir los privilegios de usuario, registro de Huellas digitales y Número de tarjeta, el establecimiento de contraseña y el establecimiento de privilegios de acceso.

Añadir Administrador: Elija "Administrador" en **[Privilegios de Usuario]**, quién está autorizado para operar todas las funciones en el menú.

Como se muestra a continuación, el usuario con el ID de usuario 1 es un administrador.

Agregar un Usuario Normal: Elija "Usuario Normal" en [Privilegios de usuario]. Cuando ya se estableció un administrador, los usuarios normales sólo pueden utilizar huella digital, contraseña o tarjeta para la verificación; cuando el administrador aún no está establecido, los usuarios normales pueden controlar todas las funciones en el menú

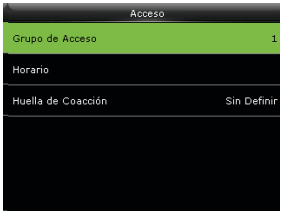
Contraseña: Se aceptan contraseñas de 1 a 8 dígitos.

Observaciones:

1. El dispositivo asigna automáticamente los ID de usuario en secuencia, pero el usuario puede configurarlo manualmente.
2. El dispositivo es compatible con IDs de usuarios de 1 a 14 dígitos.

4.2 Configuración de Privilegio de Acceso

La opción de Privilegio de Acceso de los usuarios se usa para configurar el acceso a la puerta, incluyendo los ajustes de grupos de acceso, horarios de tiempo para acceder y la configuración de las huellas digitales de coacción.



Grupo de Acceso: Sirve para asignar a los usuarios a diferentes grupos de control de acceso y así crear combinaciones de acceso multi-usuario. Los nuevos usuarios pertenecen a Grupo 1 en la por defecto, y pueden ser reasignados a otros grupos.

Horario: Seleccione los horarios para el usuario. Los horarios se establecen en el menú de Acceso y un máximo de 50 horarios son compatibles. El tiempo efectivo de apertura de la puerta para un usuario es la suma de los horarios seleccionados.

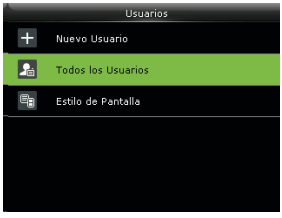
Huellas Digitales de Coacción: El usuario puede elegir una o más huellas digitales registradas como huellas de coacción. Cuando se verifica con esa huella digital, se activará la alarma de coacción.

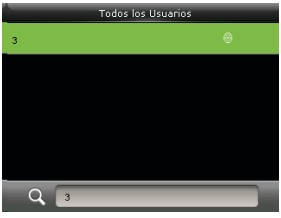
Usuarios

Ejemplo: Entre las huellas digitales registradas (6, 7, 8), elija la 8º como la huella digital de coacción.

4.3 Buscar Usuario

Introduzca el ID de usuario en la lista **[Todos los Usuarios]** para buscar un usuario.





En la Interfaz, presione → > **Usuarios** >**Todos los Usuarios** para entrar en la Interfaz de Todos los Usuarios. Introduzca el nombre o ID de usuario en la casilla de búsqueda y aparecerá el usuario correspondiente, Como se muestra en la figura anterior, busque al usuario con el ID de usuario "2".

Para introducir el nombre, consulte 17.1 Instrucciones para Introducir de Texto

4.4 Editar Usuario

Después de elegir un usuario a través de 4.3 Buscar Usuarios, presione ⏎ y seleccione **[Editar]** para entrar en la interfaz de edición de usuario.

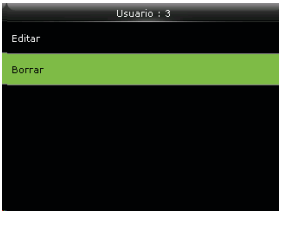
O desde la interfaz inicial presione ⏎ >**Usuarios** > **Todos los usuarios** > Busque un usuario> Presione ⏎ > **Editar** para entrar en la interfaz de edición de usuario.

El método de operación de edición de usuario es el mismo que el de agregar usuario, pero el ID de usuario no se puede editar.

4.5 Eliminar Usuario

Después de elegir un usuario a través de 4.3 Buscar Usuarios, presione ⏎ y seleccione **[Borrar]** para entrar en la interfaz de eliminación de usuario.

O desde la interfaz inicial presione ⏎ >**Usuarios** > **Todos los usuarios** > Busque un usuario> Presione ⏎ > **Borrar** para entrar en la interfaz de eliminación de usuario.



Usuarios

Nota: Sólo cuando el usuario haya registrado huella digital, contraseña o tarjeta, se mostrará el elemento en la lista para su eliminación.

4.6 Estilo de Pantalla

En la interfaz inicial, presione > **Usuarios** > **Estilo de pantalla** para entrar en la interfaz de configuración de Estilo de Pantalla.

A continuación, se muestran los diferentes estilos de pantalla.

Linea Simple

Línea Múltiple

Línea Mixta

Privilegios de Usuario

Se configuran los permisos de operación del menú que puede tener un usuario (Se pueden configurar un máximo de 3 perfiles de privilegios). Cuando los Privilegios de Usuarios están habilitados, en [**Usuarios**]> [**Nuevo Usuario**] > [**Privilegios**], puede asignar los privilegios adecuados a cada usuario.

Privilegios: El Administrador puede asignar diferentes permisos a los nuevos usuarios. Para evitar tener que establecer permisos para cada usuario uno por uno, usted puede configurar perfiles de privilegios para categorizar diferentes niveles de permisos en la gestión de usuarios.

5.1 Habilitar Privilegios de Usuario

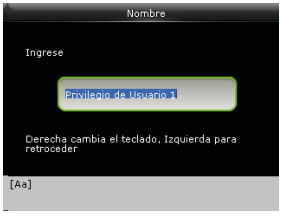
En la interfaz inicial, pulse [M] > **Privilegios** > **Privilegio de Usuario 1 (2/3)**> **Activar Privilegio**, presione [M] para activar el privilegio.

Después de activar privilegios, puede asignar estos privilegios en [**Usuarios**]> [**Nuevo usuario**]> [**Privilegios de Usuario**].

Observaciones: Se requiere de al menos un administrador registrado para activar los privilegios de usuario.

Privilegios de Usuario

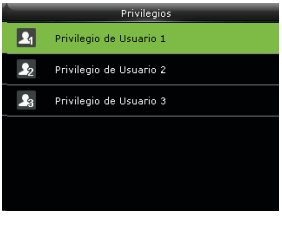
5.2 Introducir nombre del Permiso

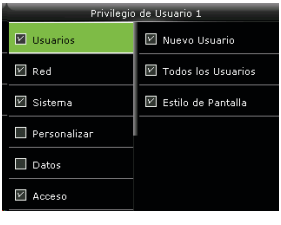


En la interfaz inicial, presione [M] > **Privilegios** > **Privilegio de Usuario1 (2/3)**> Nombre para entrar en la interfaz de edición. Introduzca un nombre usando el teclado T9, presione [M] para guardar los ajustes y regresar a la interfaz anterior.

Para más detalles sobre cómo introducir el nombre, consulte 17.1 Instrucciones para Introducir Texto.

5.3 Asignación de Permisos

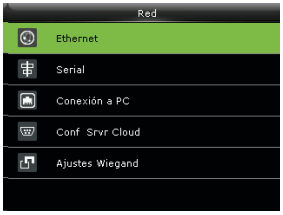


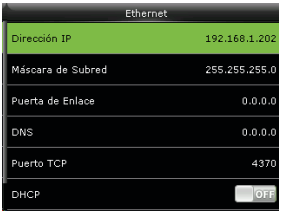


En la interfaz inicial, presione [M] > **Privilegios** > **Privilegio de Usuario1 (2/3)**> **Definir Privilegios** para entrar en la interfaz de asignación de privilegios. Presione [M] para seleccionar o deseleccionar los permisos de operación de cada menú para un perfil de privilegios.

Ajustes de Red

6.1 Configuración de Ethernet





En la interfaz inicial, presione > **Red** > **Ethernet** para entrar en la interfaz de Configuración de Ethernet.

Los parámetros siguientes son los valores predeterminados de fábrica, por favor, ajuste de acuerdo a la situación real de la red.

Dirección IP: 192.168.6.201

Máscara de Subred: 255.255.2550

Puerta de enlace: 0.0.0.0

DNS: 0.0.0.0

Puerto TCP: 4370

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

Mostrar en la barra de estado: Para establecer si se muestra el ícono de red en la barra de estado.

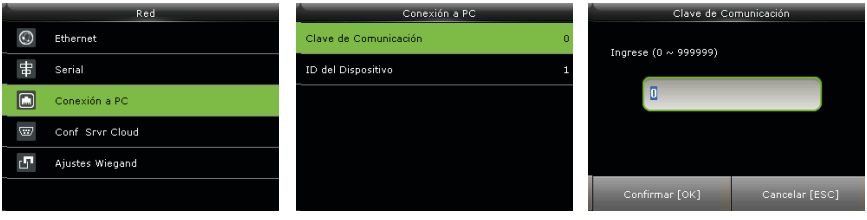
Ajustes de Red

6.2 Conexión a PC

- Configuración de Clave de Comunicación

Para mejorar la seguridad de los datos, una **Clave de Comunicación** entre el dispositivo y el PC necesita ser establecida.

Si una Clave de Comunicación se establece en el dispositivo, la contraseña de conexión se debe introducir cuando el dispositivo se conecte al software de PC, de forma que el dispositivo y el software puedan comunicarse.



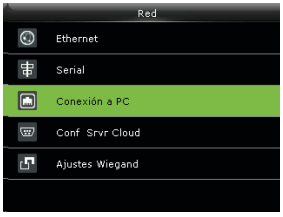
En la Interfaz inicial, pulse → > **Red** > **Conexión a PC**> **Clave de Comunicación**

Clave de Comunicación: La contraseña por defecto es 0 (No hay clave). La Clave de Comunicación puede tener de 1 a 6 dígitos y oscilar entre 0 ~ 999999.

- Configuración del ID del Dispositivo.

Si el método de comunicación es RS485, se requiere introducir el ID del Dispositivo en la interfaz de comunicación con el software.

Ajustes de Red



En la interfaz inicial, presione ⏎ > **Red** > **Conexión a PC**> **ID del Dispositivo**

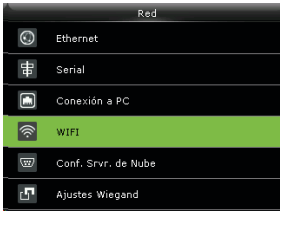
ID del Dispositivo: Número de identificación del dispositivo, que oscila entre 1 ~ 254.

6.3 Conexión Inalámbrica *

El dispositivo tiene integrado un módulo Wi-Fi para lograr una conexión inalámbrica a la red.

- Conexión Wi-Fi

En la interfaz inicial presione ⏎ para entrar al menú principal y seleccione **RED.**



Presione ▼ para seleccionar Red Inalámbrica y presione ⏎

Presione ⏎ para activar el WI-Fi, el dispositivo buscará las redes inalámbricas cercanas.

Ajustes de Red

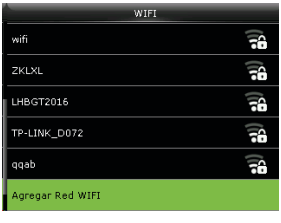
Seleccione una red Wi-Fi disponible, presione → para entrar a la interfaz de ingreso de contraseña, introduzca la contraseña y presione →

Conectando…

Cuando se conecte a la red Wi-Fi, se mostrará el logo en la interfaz inicial.

- Agregar red Wi-Fi de forma manual

Puede agregar manualmente una red Wi-Fi cuando no se muestre en la lista la red a la que desea conectarse.



Presione ▼ para seleccionar "Agregar Red Wi-FI" y presione → .

Introduzca la información necesaria (la red Wi-Fi debe existir).

Ajustes de Red

Observaciones:

Después de agregar la red Wi-FI de forma manual, encuentre el nombre de la red en la lista de redes. Para conectarse a la red, consulte la sección Conexión Wi-Fi.

- Ajustes Avanzados

Presione ▼ para seleccionar "Avanzado" y presione

Introduzca la información necesaria según lo requiera.

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

Dirección IP: La dirección IP para la red Wi-Fi, por defecto es 0.0.0.0, lo puede modificar de acuerdo a la situación actual de la red.

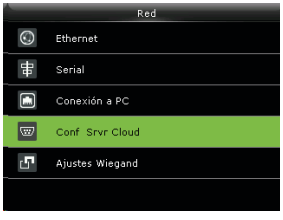
Máscara de Subred: Por defecto es 255.255.255.0, lo puede modificar de acuerdo a la situación actual de la red.

Puerta de enlace: Por defecto es 0.0.0.0, lo puede modificar de acuerdo a la situación actual de la red.

Observaciones: La función Wi-Fi es opcional, contacte a su técnico de ventas si requiere esta función.

Ajustes de Red

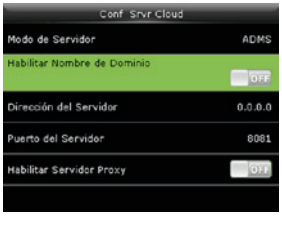
6.4 Configuración de Servidor en la Nube



En la interfaz inicial, presione > **Red** > **Conf. de Srvr Cloud.**

6.4.1 ADMS

Ajustes utilizados para la conexión con el servidor ADMS, como la dirección IP, configuración del puerto, y si conviene habilitar el servidor proxy, etc.



Cuando el servidor web está conectado correctamente, la interfaz principal mostrará el logo .

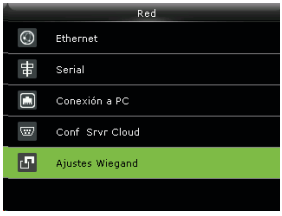
Habilitar nombre de Dominio: Cuando se activa esta función, el nombre de dominio en forma "http://..." se usará, por ejemplo http://www.XXX.com. Donde XXX denota el nombre del dominio cuando esta función esta activada; cuando esta desactivada, introduzca la dirección IP en XXX.

Dirección del Servidor: Introduzca la dirección IP del servidor ADMS.

Puerto del Servidor: Introduzca el número de puerto utilizado por el servidor ADMS.

Habilitar Servidor Proxy: Método para permitir proxy. Para habilitar el Proxy, configure la dirección IP y número de puerto del servidor proxy. La forma de introducir la IP del Proxy y la dirección del servidor es la misma.

6.5 Ajustes Wiegand



En la interfaz inicial, presione > **Red** > **Ajustes Wiegand**

6.5.1 Entrada Wiegand

La conexión de entrada Wiegand es compatible con lectores de tarjetas, o conecta el dispositivo como un dispositivo maestro a otro dispositivo (dispositivo esclavo), formando un sistema maestro / esclavo.

Seleccione "Entrada Wiegand" para ajustar los parámetros en la interfaz de Entrada Wiegand.

Ajustes de Red

Formato Wiegand: Los usuarios pueden elegir entre los formatos wiegand incorporados en el sistema: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a, Wiegand 50 y **Ninguno**. El valor ninguno significa que el formato con este número no se usa. La siguiente tabla describe todos los formatos.

Ancho 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 entrada incluido en la señal de entrada Wiegand. Se puede elegir entre ID de Usuario o Número de Tarjeta.

Definiciones de los formatos Wiegand:

Formato Wiegand	Descripción
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCO 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.

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	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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.

Ajustes de Red

Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.	

6.5.2. Salida Wiegand

La conexión de salida Wiegand sirve para conectar el dispositivo como un dispositivo esclavo a otro dispositivo (dispositivo maestro), formando un sistema esclavo/maestro.

Seleccione "Salida Wiegand" para ajustar los parámetros en la interfaz de Salida Wiegand.

Formato Wiegand: Los usuarios pueden elegir entre los formatos wiegand incorporados en el sistema: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a and Wiegand 50. Aunque se soportan varios formatos, el formato real está determinado por los Bits de Salida 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 que se usará será Wiegand36 de 36 bits.

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

ID por Verificación 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 Sitio: 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.

Ajustes de Red

Ancho 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.

6.5.3 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 detectará el número de la misma de acuerdo a todos los 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.

En la interfaz inicial, presione > **Red** > **Configuración Wiegand** > **Detección Automática de Formato de Tarjeta.**

Ajustes de Red

Procedimiento de la Operación:

1. Después de entrar a la interfaz de **Detección Automática de Formato de Tarjeta,** deslice la tarjeta de identificación sobre el lector de tarjetas (ya sea en el mismo dispositivo o en el lector de tarjetas auxiliar), la interfaz mostrará los formatos wiegand detectados automáticamente y los números de tarjeta analizados.

2. Elija el elemento que corresponda al número real de la tarjeta y establézcalo como el **Formato Wiegand** del dispositivo. Este es el formato necesario para leer el tipo de tarjeta presentada.

Observaciones: En la interfaz de Detección Automática de Formato de Tarjeta de un dispositivo IC, el dispositivo no puede detectar el número de la tarjeta o el formato wiegand solamente deslizando una Tarjeta ID. Para detectar el formato wiegand de una Tarjeta ID, es necesario conectar un lector de tarjetas IC al dispositivo y deslizar la tarjeta en el lector auxiliar.

Control de Acceso

La opción Control de Acceso se usa para establecer todos los parámetros relacionados al control de la cerradura u otros dispositivos, así como para establecer horarios, días festivos, verificaciones combinadas, etc.

En la interfaz inicial, presione > **Acceso.**

Para poder acceder, el usuario registrado debe cumplir las siguientes condiciones:

1. La hora de acceso del usuario debe estar dentro del horario personal del usuario o en el horario de su grupo.
2. El grupo del usuario debe estar dentro de la combinación de acceso multi-usuario (cuando hay otros grupos en la misma combinación de acceso, se requiere la verificación de los miembros de esos grupos para poder abrir la puerta).

En las configuraciones predeterminadas, los usuarios nuevos son asignados en el primer grupo de acceso con el horario de grupo predeterminado [1] y combinación de acceso "1", además quedan en estado desbloqueado.

7.1 Opciones de Control de Acceso

En la interfaz inicial, presione > **Acceso** > **Opciones de Acceso.**

Control de Acceso

- Retardo de la cerradura (s): 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 (s): 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 1 a 255 segundos).

- Tipo de Sensor de Puerta: Incluye **Normalmente Abierto (N.O.)**, **Normalmente Cerrado (N.C.)** 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.

- Método de Verificación: Seleccione el método de verificación para abrir la puerta. Los métodos son: Contraseña/Huella/Tarjeta, Sólo Huella, Sólo ID de Usuario, Contraseña, Sólo Tarjeta, Huella/Contraseña, Contraseña/Tarjeta, ID de Usuario & Huella, Huella & Contraseña, Huella & Tarjeta, Huella & Contraseña & Tarjeta, Contraseña & Tarjeta, ID de Usuario & Huella & Contraseña, Huella & Tarjeta & ID de Usuario.

Observaciones:

1. / Significa "O". & Significa "Y".
2. En un método de multi-verificación, la información de verificación correspondiente debe ser registrada primero. Por ejemplo: Cuando el usuario A presenta sólo su huella digital, pero el método de verificación seleccionado es "Contraseña & Tarjeta", el usuario A no pasará la verificación.

Control de Acceso

- Horario de Puerta Habilitada Establece periodos para que los usuarios abran la puerta.

- Horario de Normalmente Abierto: Establece el periodo de tiempo para el modo Normalmente Abierto, de forma que la puerta siempre esté abierta durante este periodo.

- Usar como Maestro: Al configurar los dispositivos maestros y esclavos, puede establecer el estado del dispositivo maestro como Salida o Entrada.

Salida: Una verificación en el dispositivo maestro es un registro de salida.
Entrada: Una verificación en el dispositivo maestro es un registro de entrada.

- 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: Para reiniciar los parámetros de Retardo de la Cerradura, Retardo del Sensor de Puerta, Tipo de Sensor de Puerta, Método de Verificación, Periodo de Tiempo de Puerta Disponible, Periodo de Tiempo N.O., Configuración de Entrada Auxiliar, Alarma de Altavoz, Dirección de Anti-Passback. Sin embargo, el contenido de "Borrar Datos" en el menú [Datos] no se verá afectado.

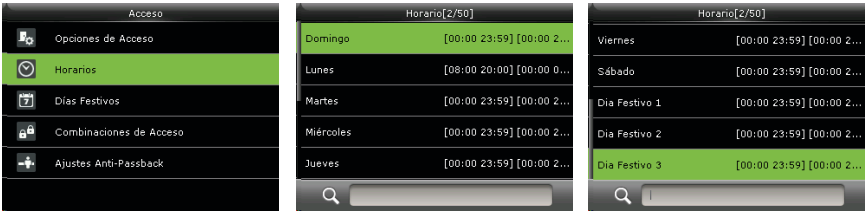
Parámetros de Acceso	Valor de Fábrica
Retardo de la cerradura	5 s
Retardo de sensor de puerta	10 s
Tipo de Sensor de la Puerta	Normalmente Abierto (NO)
Método de Verificación	Contraseña/Huella Digital/Tarjeta
Periodo de Tiempo de Puerta Disponible	1
Periodo de Tiempo NO	Ninguno
Usar como Maestro	Entrada
Alarma de Altavoz	Apagado
Dirección de Anti-Passback	Sin Anti-passback

Observaciones:
Después de establecer un Horario Normalmente Cerrado, cierre bien la puerta, de lo contrario, podría activarse la alarma durante el Horario Normalmente Cerrado.

7.2 Ajustes de Horarios

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 3 secciones de días festivos, y cada sección de tiempo contiene el periodo válido dentro de 24 horas.

Usted puede establecer un máximo de 3 periodos de tiempo para cada sección de tiempo. La relación entre estos periodos de tiempo es "O". Cuando la hora de una verificación cae dentro de cualquiera de estos periodos de tiempo, la verificación es válida.

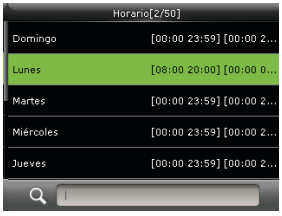


El formato del periodo de tiempo es HH:MM-HH:MM en el sistema de 24 horas con precisión de minutos.

En la interfaz inicial, presione > **Acceso** > **Horarios** para entrar en la interfaz de **Ajustes de Horarios**. El número de horario predeterminado es 1 (válido todo el día), y no se puede editar.

-Editar un Horario

Un administrador puede editar un horario según sea necesario. La operación es la siguiente:



Introduzca un número de Horario (como "2") en la barra de búsqueda. El horario (2) se seleccionará automáticamente. Seleccione una sección de tiempo (como "lunes") y presione ⏎

Seleccione "Horario 1/2/3" y presione ⏎ para entrar a la interfaz de ajuste de periodo de tiempo

Establezca la "Hora de inicio" y "Hora de fin" como lo requiera, después presione ⏎ para guardar y salir.

Operación: Puedes establecer la hora de inicio y hora de fin presionando ▲/▼ o escribirla directamente, presione ◄/► para cambiar de casilla de edición.

Usted puede establecer otras secciones de tiempo según sea necesario, después de configurar la sección de tiempo para lunes, presione ⏎ para salir.

Nota:

(1) Cuando la hora de fin es más temprana que la hora de inicio (por ejemplo, 23:57-23:56), quiere decir que se mantiene cerrado todo el día. Cuando la hora de fin es más tarde que la hora de inicio (por ejemplo, 00:00-23:59), quiere decir que este periodo de tiempo es válido.

(2) **Horario Válido:** 00:00-23:59 (Válido todo el día) o cuando la hora de fin es mas tarde que la hora de inicio (por ejemplo: 08:00-23:59).

(3) De forma predeterminada, el Horario 01 indica validez de todo el día (00:00-23:59).

7.3 Ajustes de Días Festivos

Usted puede agregar días festivos al dispositivo de control de acceso y establecer los periodos de tiempo para dichos días festivos según sea necesario.

En la interfaz inicial, presione > **Acceso** > **Días Festivos.**

7.3.1 Agregar Día Festivo

Seleccione "Agregar Día Festivo" y presione para entrar.

Seleccione "Fecha" y presione para entrar.

Establezca la fecha para el día festivo, presione para guardar y salir.

Los parámetros de día festivos son los siguientes:

Número: El dispositivo automáticamente asigna un número a un día festivo. También puede seleccionar **Número** y presionar para entrar a la interfaz de Número. Introduzca el número de un día festivo y presione para guardar los ajustes y regresar a la interfaz de Días Festivos.

Nota: El número de un día festivo puede variar de 1 a 24.

Control de Acceso

Fecha: Establezca la fecha de un día festivo. Presione ▲/▼ o escriba directamente la fecha, presione ◄/► para cambiar de casilla de edición, luego presione [→] para guardar los cambios y regresar a la interfaz de **Días Festivos.**

Tipo de Día Festivo: Puede clasificar el día festivo en 3 tipos (1/2/3). El periodo de tiempo válido para cada tipo de día festivo se puede editar en la interfaz de Ajustes de Horario. Para más detalles sobre editar horarios, consulte la sección 7.2 Ajustes de Horario.

Repetir: El valor predeterminado de "Repetir" es Encendido **[ON]**. Puede presionar [→] para cambiar entre Encendido **[ON]** y Apagado **[OFF].**

Para días festivos fijos de cada año, por ejemplo, Año Nuevo el 1º de Enero, "Repetir o no" puede activarse". Para días festivos no fijos de cada año, por ejemplo, el Día de las Madres en el segundo domingo de Mayo (depende del país), no hay una fecha fija por lo que "Repetir o no" puede desactivarse.

Por ejemplo, cuando la fecha de un día festivo se establece para 1º de Enero de 2016 y el tipo de día festivo se establece en 1, el control de acceso para el 1º de enero se lleva a cabo de acuerdo al periodo de tiempo establecido para los Días Festivos Tipo 1 en vez del periodo de tiempo establecido para el viernes.

7.3.2 Todos los Días Festivos.

Presione ▼ para seleccionar "Todos los Días Festivos" y presione [→] para entrar.

Seleccione un día festivo y presione [→] para entrar

Edite o borre el día festivo.

Observaciones:
Los métodos para editar o borrar un día festivo son iguales a los usados para editar o borrar un usuario por lo que no se describen aquí. Para más detalles, consulte la sección 4.4 Editar Usuario y 4.5 Eliminar Usuario.

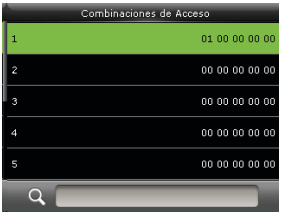
7.4. Ajustes de Combinaciones de Acceso

Combine 2 o más grupos de acceso para crear una verificación multi-usuario y así aumentar la seguridad.
En la Combinación de Acceso, se pueden combinar hasta 5 usuarios; todos los usuarios pueden pertenecer a un mismo grupo de acceso o a hasta 5 grupos diferentes.

Los grupos de acceso se asignan cuando se agrega un usuario (en la interfaz inicial, presione [→] > Usuarios > Nuevo Usuario > Privilegios de Acceso > Grupo de Acceso). En la Combinación de Acceso puede seleccionar los grupos de acceso a combinar.

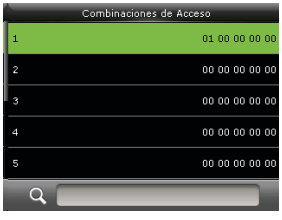
Observaciones: Si a un usuario se le asigna un grupo de acceso que no existe en ninguna Combinación de Acceso, el usuario no podrá acceder a la puerta.

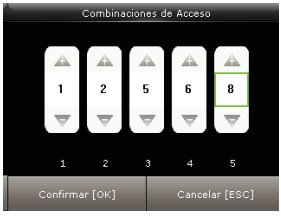
Control de Acceso

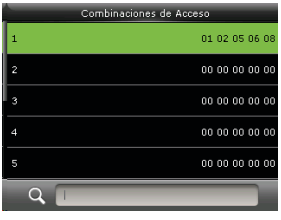


En la interfaz inicial, presione > **Acceso** > **Combinaciones de Acceso** > **1** para entrar en la interfaz de la primera Combinación de Acceso.

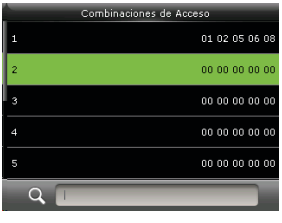
Por ejemplo:

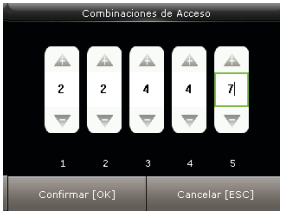


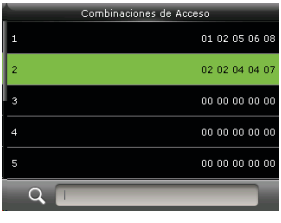




En la figura anterior, la Combinación de Acceso 1 está compuesta de cinco miembros de cinco grupos de acceso diferentes --- Grupo de acceso 1, 3, 5, 6, 8 respectivamente.

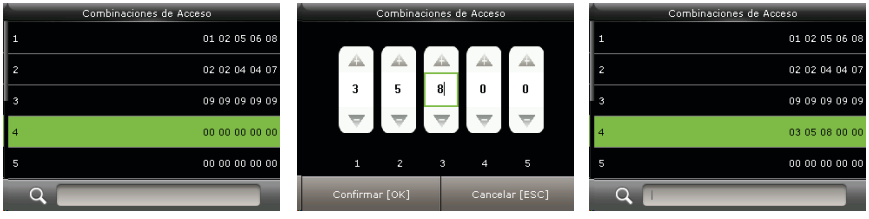






En la figura anterior, la Combinación de Acceso 2 está compuesta de cinco miembros de tres grupos de acceso diferentes: dos miembros del grupo de acceso 2, dos miembros del grupo de acceso 4 y un miembro del grupo de acceso 7.

En la figura anterior, la Combinación de Acceso 3 está compuesta de cinco miembros, todos ellos del grupo de acceso 9.



En la figura anterior, la Combinación de Acceso 4 está compuesta de tres miembros de tres grupos de acceso diferentes --- Grupos de acceso 3, 5, 8 respectivamente.

Eliminar una Combinación de Acceso

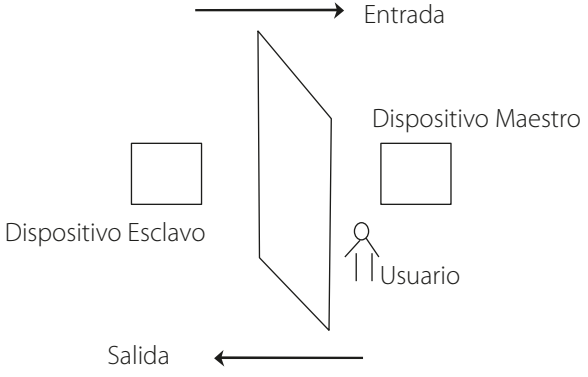
Para eliminar una Combinación de Acceso, establece todos los números de grupos de acceso a 0.

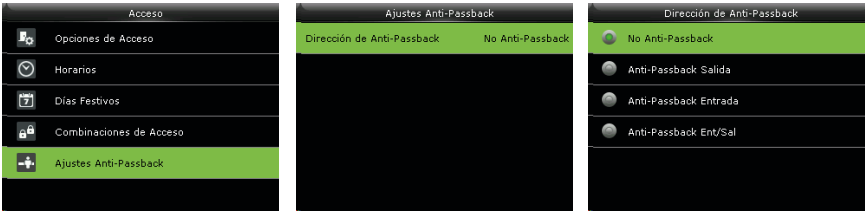
Por ejemplo, para eliminar la Combinación de Acceso 4, por favor observe las siguientes figuras:

Si todos los números de grupos de acceso de la Combinación de Acceso 4 se establecen a 0, la combinación queda eliminada.

7.5 Ajustes Anti-Passback

Para evitar que una persona que sigue a un usuario consiga acceder sin verificación, lo cual resulta en un problema de seguridad, los usuarios pueden activar la función Anti-Passback. Bajo esta función el registro de entrada debe coincidir con el registro de salida para poder abrir una puerta.
Esta función requiere de 2 dispositivos trabajando juntos: Uno instalado dentro de la puerta (dispositivo maestro) y otro instalado fuera de la puerta (dispositivo esclavo). Ambos dispositivos se comunican a través de una señal Wiegand.
El formato Wiegand y el tipo de salida (ID de Usuario/Número de Tarjeta) de ambos dispositivos debe ser consistente.





En la interfaz inicial, presione > **Acceso** > **Ajustes Anti Passback**

- Dirección de Anti-Passback

No Anti-Passback: La función Anti-Passback está desactivada, lo que significa que la verificación, ya sea en el dispositivo maestro o esclavo, puede abrir la puerta. Los registros de acceso no se guardan.

Anti-Passback Salida: Después de que el usuario registre una salida, sólo si el registro más reciente es una entrada, el usuario puede volver a registrar una salida; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrar entradas libremente.

Anti-Passback Entrada: Después de que el usuario registre una entrada, sólo si el registro más reciente es una salida, el usuario puede volver a registrar una entrada; de lo contrario, se activará la alarma. Sin embargo, el usuario puede registrar salidas libremente.

Anti-Passback Entrada/Salida: Después de que el usuario registre una entrada/salida, sólo si el registro más reciente es una entrada, el usuario puede volver a registrar una salida, y sólo si el registro más reciente es una salida, el usuario puede volver a registrar una entrada; de lo contrario, se activará la alarma.

Configuraciones de Sistema

8.1 Ajustes de Registros de Acceso

En la interfaz inicial, presione > **Sistema** > **Ajustes de Eventos de Acceso.**

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.

Borrar Eventos Antiguos: La cantidad de registros de acceso que 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.

Mostrar Confirmación (s): El tiempo que se muestra en la pantalla el resultado de las verificaciones. El valor oscila de 1 a 9 segundos.

Tamaño de letra de Verificación: Puede elegir el tamaño de letra del mensaje de resultado de verificación.

8.2 Ajustes de Huella Digital

En la interfaz inicial, presione > **Sistema** > **Huella**.

Configuraciones de Sistema

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

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

Sensibilidad del Sensor: 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"**.

Detección de dedo vivo: Definir si se utiliza la función anti-huellas falsas. Cuando esta herramienta está activada y se están 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.

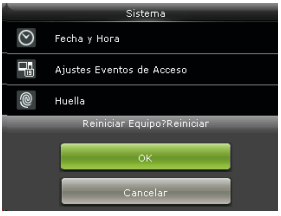
Intentos en Modo 1:1 : Este parámetro es utilizado para establecer el número de reintentos en el caso de que ocurran errores durante la verificación 1:1 ya sea de huella o contraseña. Para evitar tener que volver a escribir el ID del usuario, se permiten los reintentos. El número de reintentos puede oscilar entre 1 a 9.

Imagen de Huella: Esta función determina si desea mostrar la imagen de la huella digital durante el registro o verificación de estas. Hay 4 opciones disponibles: Mostrar en registro, Mostrar en Verificación, Siempre mostrar, No mostrar.

8.3 Reestablecer Valores de Fábrica.

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

Configuraciones de Sistema



En la interfaz inicial, presione > **Sistema** > **Reiniciar Equipo** > **OK** para reestablecer los valores de fábrica.

Los ajustes que se reestablecen incluyen las opciones de Control de Acceso, Opciones de Coacción, configuraciones Anti-passback, configuraciones de Red (esto es, las configuraciones ethernet, comunicación serial, Conexión a PC y configuraciones Wiegand), Configuraciones de Personalización (como Voz, Sonido del Teclado, Volumen y Tiempo de Espera para Reposo) etc.

Parámetros	**Valores de Fábrica**
Opciones de Control de Acceso	Retardo de Cerradura: 10 Segundos Retardo de Sensor de Puerta: 10 Segundos Tipo de Sensor de Puerta: Normalmente Abierta (NO) Retraso de Alarma de Puerta: 30 Segundos Intentos para Activar Alarma: 3 intentos Periodo de Tiempo NC: Ninguno Periodo de Tiempo NO: Ninguno Días Festivos Válidos: Apagado Alarma: Apagada
Opciones de Coacción	Función de Coacción: Apagado Alarma en Verificación 1:1: Apagado Alarma en Verificación 1:N: Apagado Alarma con Contraseña: Apagado Retraso de Alarma: 10 Segundos
Dirección de Anti-Passback	Sin Anti-Passback
Ethernet	Dirección IP: 192.168.6.192 Máscara de Subred: 255.255.255.0 DNS: 0.0.0.0
Conexión a PC	Clave de Comunicación: 0 ID de Dispositivo: 1

ADMS	Habilitar Nombre de Dominio: Apagado Dirección de Servidor: 0.0.0.0 Puerto de Servidor: 8081 Habilitar Servidor Proxy: Apagado
Configuración Wiegand	Tipo de ID de Entrada/Salida Wiegand: Número de Tarjeta Ancho de Pulso: 100 us Intervalo de Pulso: 1000 us
Tiempo de Espera para Diapositivas	60 segundos
Tiempo de Espera para Reposo	30 minutos
Tiempo de Espera del Menú	60 segundos
Sonido del Teclado	Activado
Sonido de Voz	Activado
Volumen	70

Observaciones:
Al reestablecer a los valores de fábrica, la hora y fecha no se verán afectadas. Por ejemplo, si la fecha y hora del dispositivo es 18:30 del 1 de enero de 2020, la fecha y hora se mantendrá igual después de reestablecer los valores de fábrica.

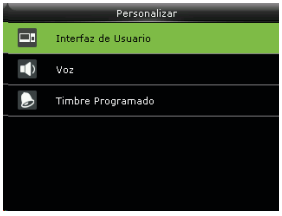
8.4. Actualización por USB

Inserte la Unidad USB con el archivo de actualización en el puerto USB del dispositivo, y en la interfaz inicial presione > **Sistema** > **Actualización por USB** para completar la operación de actualización de firmware.

Si necesita un archivo de actualización, póngase en contacto con nuestro soporte técnico.
La actualización de Firmware no se recomienda bajo circunstancias normales.

Configuraciones de Personalización

9.1 Ajustes de Interfaz de Usuario



En la interfaz inicial, presione > **Personalizar** > **Interfaz de Usuario**.

Fondo de Pantalla: Seleccione la imagen a utilizar como fondo de pantalla, puedes encontrar varios estilos dentro del dispositivo.

Idioma: Seleccione el idioma del dispositivo.

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

Observaciones:
Si se desactiva esta opción, el sistema no regresará a la interfaz inicial cuando no haya ninguna operación. No se recomienda desactivar esta función debido al alto consumo de energía y a que representaría un problema de seguridad.

Iniciar Protector de Pantalla (s): Cuando no se haga ninguna operación en la interfaz inicial después del periodo de tiempo seleccionado, iniciará un protector de pantalla. Esta opción puede desactivarse (elija "Ninguno") o establecerse entre 3 a 999 segundos.

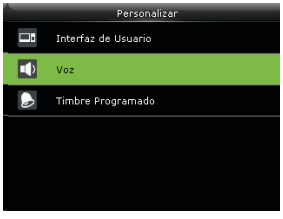
Intervalo de Imágenes (s): Se refiere al intervalo de tiempo entre dispositivas diferentes. Puede desactivarse o establecerse entre 3 a 999 segundos.

Tiempo para Reposo (m): Esta función permite establecer el tiempo de espera del dispositivo para ingresar al modo de reposo. Presione cualquier tecla para sacar al dispositivo del estado de reposo. El rango de espera es de 1 a 999 minutos. Esta función se puede desactivar.

Observaciones: No se recomienda desactivar esta función debido al alto consumo de energía.

Estilo de la Pantalla Principal: Seleccione la posición y forma del reloj y de las teclas de estado de la pantalla inicial.

9.2 Ajustes de Voz



En la interfaz inicial, presione [M] > **Personalizar** > **Voz**

Voz: Seleccione si desea activar los mensajes de voz durante la operación del dispositivo. Presione [M] para activarlo.

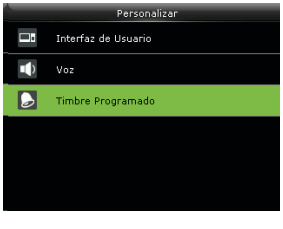
Sonido de Teclas: Seleccione si desea activar el sonido al tocar el teclado. Presione [M] para activarlo.

Volumen: Ajuste el volumen del dispositivo. El valor predeterminado es 70. Presione **>** para incrementar el volumen, presione **<** para disminuirlo.

9.3 Ajustes de 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.

9.3.1 Agregar un Timbre



En la interfaz inicial, presione [M] > **Personalizar** > **Timbre Programado** > **Nuevo Horario de Timbre.**

Configuraciones de Personalización

Estado del Timbre: ON es para activar el timbre, **OFF** es para desactivarlo.

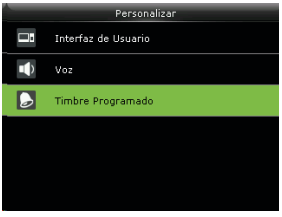
Hora de Timbre: El timbre suena automáticamente cuando se llega a la hora especificada.

Repetir: Establecer si el timbre se repite de lunes a domingo.

Tono: El tono que suena como timbre.

Duración del Timbre: Para establecer la duración del timbre. El valor oscila entre 1 a 999 segundos.

9.3.2 Editar un Timbre



Presione **V** para seleccionar "Timbres Programados" y presione

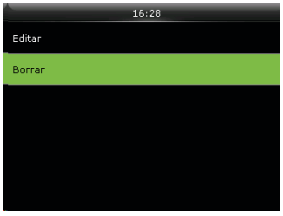
Presione **V** para seleccionar "Horarios de Timbre" y presione

Seleccione el timbre que desea editar y presione

Seleccione "Editar" y presione

Modifique los parámetros del timbre.

9.3.3 Borrar un Timbre



Presione ▼ para seleccionar "Borrar" y luego presione ⏎

Presione Λ para seleccionar "SI" y luego presione ⏎ para borrar el timbre.

Gestión de Datos

10.1 Borrar Datos

Aquí puede gestionar los datos en el dispositivo, que incluye borrar registros de eventos, borrar todos los datos, borrar privilegios de administrador, borrar protectores de pantalla, etc.

En la interfaz inicial, presione [M] > **Datos** > **Borrar Datos.**

Borrar Eventos de Acceso: Eliminar todos los registros de acceso guardados en el dispositivo o borrar registros de acceso de un rango de tiempo específico.

Borrar Todo: Eliminar toda la información de los usuarios, huellas digitales, registros de acceso, etc.

Borrar Privilegios de Administrador: Convertir a todos los administradores en usuarios normales.

Borrar Control de Acceso: Borrar todos los datos de acceso.

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

Borrar Datos de Respaldo: Eliminar todos los datos de respaldo.

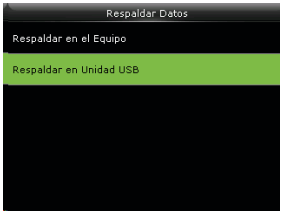
10.2 Respaldo de Datos

Usted puede respaldar los datos de la empresa o datos de configuración en el dispositivo o unidad USB.

- Respaldar en Unidad USB

Inserte la unidad USB, en la interfaz inicial presione [M] > **Datos** > **Respaldar Datos** > **Respaldar en Unidad USB** > **Respaldar Contenido** > Elija el contenido que desea respaldar **(Datos del Negocio/Datos de Sistema)** > **Notas de Respaldo** (introduzca una nota de respaldo usando el teclado T9, para más

detalles sobre el ingreso de texto, consulte 17.1 Instrucciones para Introducir Texto) > **Iniciar Respaldo** para iniciar el respaldo. No es necesario reiniciar el dispositivo después del respaldo.



Observaciones: Las operaciones de Respaldar en el Dispositivo son iguales a las de Respaldar en Unidad USB.

10.3 Restaurar Datos

Para restaurar datos guardados en el dispositivo o en una unidad USB al dispositivo.

-Restaurar desde unidad USB

Inserte la unidad USB, en la interfaz inicial presione > **Datos** > **Restaurar Datos** > **Restaurar desde Unidad USB** > **Contenido** > Elija el contenido que desea restaurar **(Datos del Negocio/Datos de Sistema)** > **Notas** (introduzca una nota usando el teclado T9, para más detalles sobre el ingreso de texto, consulte 17.1 Instrucciones para Introducir Texto) > **Iniciar Restauración** > Seleccione **Sí** para iniciar la restauración. Cuando finalice la restauración, haga clic en **[OK]** para reiniciar el dispositivo automáticamente.

Observaciones: Las operaciones de Restaurar desde el Dispositivo son iguales a las de Restaurar desde Unidad USB.

Tarjeta ID *

Para registrar una tarjeta Mifare como una tarjeta ID o como una tarjeta de huella digital. Este menú soporta la integración de asistencia con tarjetas ID y de huella digital a otros sistemas o dispositivos por medio de la tarjeta Mifare registrada, también soporta el modo de multi-verificación para satisfacer los requisitos de los clientes. También es posible limpiar la tarjeta o copiar los datos guardados en ella.

11.1 Registrar como tarjeta ID.

Registre una tarjeta Mifare como tarjeta ID. Sólo se necesita el número de ID de la tarjeta (es decir, el número ID del usuario) para registrar.

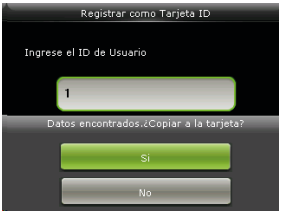
Deslizar una tarjeta Mifare registrada en el dispositivo equivale a deslizar una tarjeta ID.

En la interfaz inicial presione [→] para entrar al menú principal, luego presione > para seleccionar **Tarjeta ID** y presione [→] para entrar.

Seleccione **Registrar como Tarjeta ID** y presione [→] para entrar.

Seleccione el timbre que desea editar y presione [→]

Tarjeta ID *



Si el ID de usuario ya se ha registrado, el dispositivo preguntará si desea copiar la información a la tarjeta, y luego presione ⏎

Coloque la tarjeta en el área de tarjeta hasta que la operación sea exitosa.

- Verificación

Deslice la tarjeta Mifare registrada en el área de tarjeta. Después de que el dispositivo reconozca la tarjeta, retírela. Cuando la verificación sea exitosa, el dispositivo mostrará el número de tarjeta.

Observaciones: Modifique el Método de Verificación a uno relacionado con tarjeta en el Privilegio de Acceso de los usuarios (En la interfaz inicial, presione ⏎ > **Usuarios** > **Todos los Usuarios** > **Modo de Verificación**), o la verificación no será exitosa.

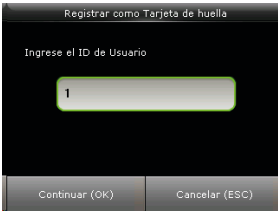
11.2 Registrar como tarjeta de Huella Digital.

Registre una huella digital y escriba los datos de la huella en la tarjeta Mifare registrada.

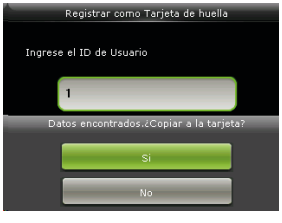
Tarjeta ID *

En la interfaz inicial presione [↵] para entrar al menú principal, luego presione > para seleccionar **Tarjeta ID** y presione [↵] para entrar

Seleccione **Registrar como Tarjeta de Huella** y presione [↵] para entrar.



Introduzca el ID de usuario que desea registrar y presione [↵]



Si el ID de usuario ya se ha registrado, el dispositivo preguntará si desea copiar la información a la tarjeta, y luego presione [↵]

Seleccione un dedo y presione [↵] , luego presione el dedo 3 veces en el lector de huellas.

Coloque la tarjeta Mifare en el área de tarjeta, espere a que el dispositivo lea los datos de la huella y retire la tarjeta hasta que la operación sea exitosa.

- Verificación

Deslice la tarjeta Mifare registrada en el área de tarjeta. Después de que el dispositivo reconozca la tarjeta, retírela. Se mostrará un mensaje pidiendo que presione su huella. Presione el dedo que registró en la tarjeta para finalizar la verificación. Si la huella presionada es diferente a la que se registró en la tarjeta, la verificación no será exitosa.

11.3 Eliminar datos de la Tarjeta

Elimine toda la información almacenada en una tarjeta Mifare.

En la interfaz inicial presione [OK] para entrar al menú principal, luego presione > para seleccionar **Tarjeta ID** y presione [OK] para entrar.

Presione ▼ para seleccionar **Eliminar Datos de la Tarjeta** y presione [OK] para entrar.

Coloque la tarjeta Mifare en el área de tarjeta, espere a que el dispositivo elimine todos los datos en la tarjeta.

Observaciones: Si los datos de la tarjeta se han guardado en el dispositivo (En la interfaz inicial presione [OK] > **Tarjeta ID** > **Todos los Usuarios** > **Opciones de Tarjeta ID** > **Modo de Almacenamiento de Datos** > Seleccione el modo "**Guardar Datos de Usuario en el Equipo**" o "**Guardar Datos de Usuario y de Huella en el Equipo**"), el dispositivo le preguntará si también desea eliminar la información guardada en el dispositivo. **[Si]** es para guardar los datos de usuario almacenados en el dispositivo. **[No]** es para conservar la información en el dispositivo.

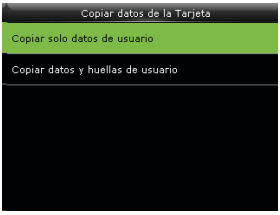
11.4 Copiar datos de la Tarjeta

Copiar la información de la tarjeta Mifare en el dispositivo (la información también se conserva en la tarjeta), de forma que pueda presionar su dedo directamente en el dispositivo sin necesidad de deslizar primero la tarjeta Mifare.

Tarjeta ID *

En la interfaz inicial presione [→] para entrar al menú principal, luego presione > para seleccionar **Tarjeta ID** y presione [→] para entrar.

Presione ▼ para seleccionar **Copiar Datos de la Tarjeta** y presione [→] para entrar.



Seleccione "Copiar sólo datos de Usuario" o "Copiar datos y huella de Usuario" y presione [→]

Coloque la tarjeta Mifare en el área de tarjetas, espere a que el dispositivo copie la información de usuario.

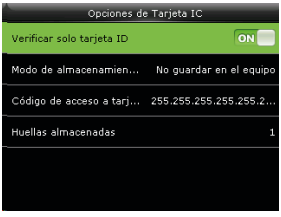
11.5 Opciones de Tarjeta ID

Establezca las opciones de la Tarjeta ID según lo requiera, como Verificar sólo tarjeta ID, Modo de Almacenamiento de Datos, Código de acceso aTarjeta y Conteo de Huellas Almacenadas.

Tarjeta ID *

En la interfaz inicial presione [OK] para entrar al menú principal, luego presione > para seleccionar **Tarjeta ID** y presione [OK] para entrar.

Presione ▼ para seleccionar **Opciones de Tarjeta ID** y presione [OK]



Establezca las Opciones de Tarjeta ID según lo requiera.

Verificar sólo Tarjeta ID: Establezca si desea verificar sólo tarjetas ID. Presione [OK] para habilitar la función. Una vez habilitada, ninguna de las tarjetas de huella digital registradas podrá verificar en este dispositivo, sólo las tarjetas ID registradas podrán hacerlo. Para más información sobre cómo registrar una tarjeta Mifare como tarjeta ID o tarjeta de huella digital, consulte las secciones 11.1 Registrar como tarjeta ID o 11.2 Registrar como tarjeta de huella digital.

Modo de Almacenamiento de Datos: Para establecer el modo de almacenamiento de los datos registrados en la tarjeta Mifare, se incluyen los siguientes modos:

1. **No guardar en el equipo:** Todos los datos registrados se guardarán sólo en la tarjeta Mifare sin guardarse en el dispositivo.
2. **Guardar Datos de Usuario en el equipo:** Se guardarán los datos de usuario sin guardar las huellas digitales en el dispositivo.
3. **Guardar Datos de Usuario y Huella en el Equipo:** Todos los datos de usuario y huella se guardarán tanto en el dispositivo como en la tarjeta Mifare.

Código de Acceso a Tarjeta: Establezca un código para la tarjeta, que puede ser de 0 a 255. Al establecer un código, el dispositivo escribirá el código en la tarjeta Mifare. La tarjeta Mifare sólo podrá usarse en este dispositivo.

Conteo de Huellas Almacenadas: Indica el número de huellas almacenadas en la tarjeta.

Gestión USB

Transfiera datos entre el dispositivo y un software correspondiente por medio de una unidad USB. Inserte una unidad USB en el puerto USB del dispositivo para subir o descargar datos.

12.1 Descargar en USB

En la interfaz inicial, presione > **Gestión USB** > **Descargar.**

Descargar Eventos de Acceso: Descargar registros de acceso de un periodo de tiempo específico en la unidad USB.

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

12.2 Cargar desde USB

En la interfaz inicial, presione > **Gestión USB** > **Cargar.**

Gestión USB

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

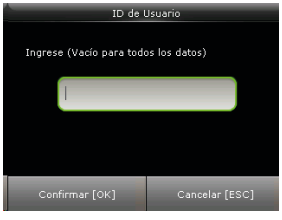
- Protector de Pantalla: Para cargar protectores de pantalla de la unidad USB al dispositivo. Durante la carga, puede seleccionar **Cargar Foto Seleccionada** o **Cargar Todas las Fotos**. Las imágenes se mostrarán en la interfaz de espera del dispositivo después de la carga. Para las especificaciones de protectores de pantalla, consulte la sección 17.4 Procedimiento para Cargar Imágenes.

- 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. Para las especificaciones de fondos de pantalla, consulte la sección 17.4 Procedimiento para Cargar Imágenes.

Búsqueda de Asistencia

Cuando los usuarios verifican exitosamente, se guarda un registro en el sistema. Esta función permite a los usuarios ver registros de asistencia.

13.1 Buscar registros de acceso



En la interfaz inicial, presione [→] > **Eventos** > **Introduzca el ID** de Usuario (si no introduce un ID, se buscarán a todos los usuarios)> Seleccione el **Periodo de Tiempo** > Presione [→] se mostrarán los registros de asistencia correspondientes.

Pruebas Automáticas

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

En la interfaz inicial, presione > **Pruebas.**

Probar Todo: Probar pantalla LCD, sonido, teclado, sensor de huellas, cámara y reloj. Durante la prueba, presione para continuar a la siguiente prueba, o presione para salir de la prueba.

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. Durante la prueba, presione para continuar a la siguiente prueba, o presione para salir de la prueba.

Probar Voz: 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. Durante la prueba, presione para continuar a la siguiente prueba, o presione para salir de la prueba.

Probar Teclado: Probar si todas las teclas funcionan correctamente. Presione cualquier tecla en la interfaz de pruebas de Teclado; si la tecla presionada coincide con el símbolo que se muestra en pantalla, la tecla funciona correctamente. Presione o para salir de la prueba.

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 pantalla. Presione o para salir de la prueba.

Probar Reloj RTC: Probar el Reloj en Tiempo Real. La terminal revisará el rendimiento del reloj examinando el cronómetro. Presione para iniciar el conteo, presione de nuevo para detenerlo y ver si el cronómetro toma el tiempo de forma precisa. Presione para salir de la prueba.

Información del Sistema

Con este parámetro usted puede ver la capacidad de almacenamiento de datos, información del dispositivo y del firmware.

En la interfaz inicial, presione > **Información.**

Capacidad del Equipo | Información del Equipo | Firmware del Firmware

Capacidad del Equipo: Muestra la cantidad de usuarios registrados, administradores, contraseñas, huellas digitales, tarjetas y eventos. También muestra la capacidad total de almacenamiento de usuarios, huellas, tarjetas y eventos.

Información del Equipo: Muestra el nombre del dispositivo, número de serie, dirección MAC, algoritmo de huella digital, información de la plataforma, versión de MCU, fabricante y fecha de fabricación.

Información de Firmware: Muestra la versión de firmware, Servicio Bio, Servicio Push* y Servicio Dev.

Observaciones: La forma en que se muestra la capacidad del dispositivo, información del dispositivo y de firmware en la interfaz de información de sistema de diferentes productos puede variar; prevalecerá el producto real.

Resolución de Problemas

- El sensor de huellas no puede de leer y verificar una huella de forma efectiva.
  - ➤ Revise si el dedo esta mojado o si el sensor de huella está mojado o polvoriento.
  - ➤ Limpie el dedo y sensor de huellas e intente de nuevo.
  - ➤ Si el dedo está muy seco, sóplele e intente de nuevo.

- Se muestra el mensaje "Horario Inválido" después de una verificación.
  - ➤ Contacte al administrador para verificar si el usuario tiene privilegio de acceder dentro de ese horario.

- La verificación se realiza con éxito, pero el usuario no puede abrir la puerta.
  - ➤ Revise si el privilegio del usuario está establecido correctamente.
  - ➤ Revise si el cableado de la cerradura es correcto.

- Suena la alarma Tamper (Anti-Sabotaje)
  - ➤ Revise si el dispositivo y la placa posterior están unidas; si no, el botón tamper en la parte trasera del dispositivo se activará y lanzará una alarma, el icono aparecerá en la esquina superior derecha de la interfaz. ⚠.

    Sólo cuando la función **[Alarma de Altavoz]** (**Acceso** > **Opciones de Acceso** > Altavoz de alarma) está activada, el altavoz lanzará una alarma.

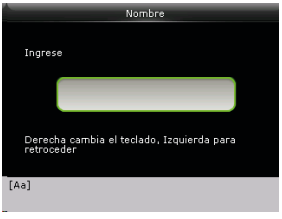
Anexos

17.1 Instrucciones para Introducir Texto

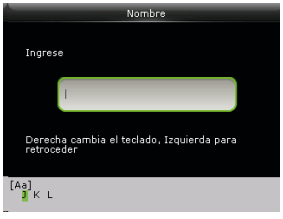
Nota: No todos los dispositivos soportan la introducción de texto con teclado T9.

Presione la tecla ► para abrir la introducción de texto y presione ► para cambiar entre los tipos de texto (Letras, Símbolo y Dígitos). Presione **ESC** para salir de la introducción de texto.

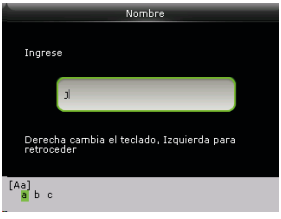
Ejemplo: Introducir el nombre "Jack"



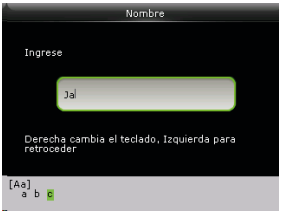
Presione la tecla ► para abrir la introducción de texto y presione de nuevo ► para cambiar al modo **[Aa]**



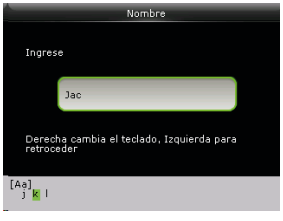
Presione una vez la tecla **5** del dispositivo para introducir la letra **J** de forma automática.



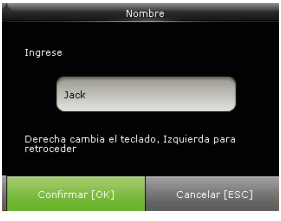
Presione dos veces la tecla **2** del dispositivo para introducir la letra **a.**



Presione tres veces la tecla **2** del dispositivo para introducir la letra **c.**

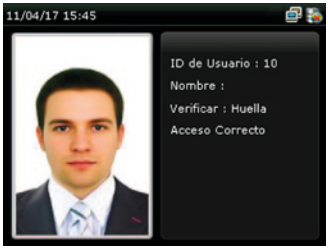


Presione una vez la tecla **5** del dispositivo para introducir la letra **k**



Después de introducir el nombre, presione para salir de la introducción de texto y presione para guardar.

17.2 Función ID con Foto*



Observaciones: Algunos modelos soportan la función ID con Foto.

Cuando la función ID con Foto está activada y el usuario verifica exitosamente, no sólo el ID y nombre del usuario se mostrarán en la pantalla, sino también la foto registrada por el usuario o guardada en la unidad USB.

Procedimiento de Operación

Se necesitan cargar las fotos de ID desde una unidad USB, el proceso de operación es el siguiente:

(1) Cree una carpeta con el nombre "photo" en la unidad USB, y guarde la foto de usuario en la carpeta.

(2) El formato de la foto debe ser JPG, y el archivo debe llamarse como el ID del usuario. Por ejemplo: La foto correspondiente al usuario con el número de ID 154 debe llamarse 154.jpg

(3) Inserte la unidad USB en el puerto USB del dispositivo, y vaya a **Gestión USB** > **Cargar** > Foto de Usuario para cargar las fotos de usuario. Ahora la foto se mostrará cada vez que el usuario verifique exitosamente.

Nota:

(1) El nombre de la foto no puede tener más de 14 dígitos.

(2) El tamaño de la foto debe ser menor a 15Kb.

(3) La nueva foto cargada reemplazará la foto original del usuario.

(4) Al descargar fotos de usuario (vaya a **Gestión USB** > **Descargar** > **Fotos de Usuario**), una carpeta llamada "photo" se creará automáticamente dentro de la unidad USB, donde se guardarán todas las fotos descargadas.

17.3 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

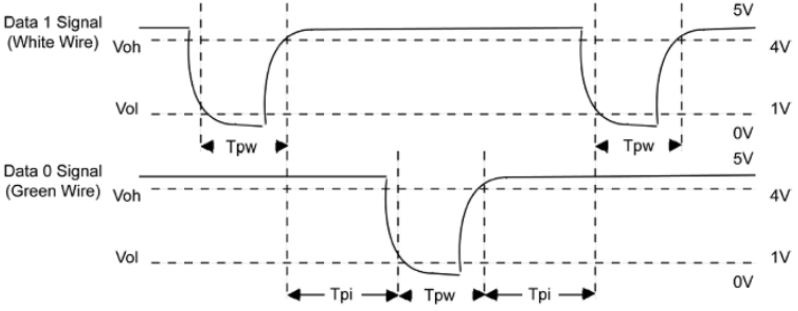
La figura 1 muestra el diagrama secuencial del lector de tarjetas que envía señales digitales en bits hacia el controlador de acceso.

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	Ancho de Pulso	100 µs
Tpi	Intervalo de Pulso	1 ms

Figura 1: Diagrama Secuencial



17.4 Procedimiento para Cargar Imágenes

1. Foto de Usuario*: Se necesita crear una carpeta llamada "**photo"** en la unidad USB y agregar las fotos de usuario dentro de esa carpeta. La capacidad es de 3000 imágenes, que no excedan los 15Kb cada una. El nombre de la imagen es x.jpg (x siendo el número de ID del usuario, máximo 14 dígitos). El formato de la foto debe ser JPG.

2. Protector de Pantalla: Se necesita crear una carpeta llamada "**advertise**" en la unidad USB y agregar las fotos a usar como protectores de pantalla dentro de esa carpeta. La capacidad es de 20 imágenes, que no excedan los 30Kb cada una. El nombre y formato de la imagen no está restringido.

3. Fondo de Pantalla: Se necesita crear una carpeta llamada "**wallpaper**" en la unidad USB y agregar las fotos a usar como fondos de pantalla dentro de esa carpeta. La capacidad es de 20 imágenes, que no excedan los 30Kb cada una. El nombre y formato de la imagen no está restringido.

17.5 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.

Anexos

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.

17.6 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
Condensado	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

www.zkteco.com

www.zktecolatinoamerica.com