MANUAL DE USUARIO

BioExterior

Controles de Acceso Independientes y
Lectores con Pantalla Blanco y Negro (Versión Profesional)

BIO TRACK

www.BioTrackSoftware.com

Contenido

1. Advertencia de uso

Gracias por usar nuestros equipos de control de acceso y lectores. Por favor lea este manual cuidadosamente para saber el funcionamiento y el modo de operación exacto de los equipos.

Deberá proteger el equipo de la exposición directa de la luz del sol debido a que esta dañará permanentemente la función del sensor de reconocimiento de huella.

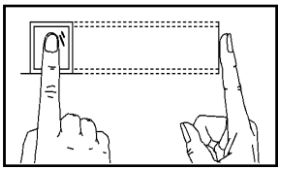
Evite el uso del producto al aire libre en verano. La temperatura de trabajo este varía desde 0 hasta 40 ° C. El calor disipado durante el funcionamiento a largo plazo puede conducir fácilmente a la desaceleración de respuesta y disminución de la verificación. Se recomienda el uso de cubiertas o dispositivos disipadores de calor para la protección del aire libre. Le recomendamos que utilice el dispositivo correctamente para lograr el efecto de reconocimiento óptimo y la velocidad de la verificación.

1. Dedos recomendados

Dedos recomendados: El índice, el de en medio o el dedo del anillo; no se recomienda usar el dedo gordo o el dedo pequeño (debido a que son torpes y difíciles de leer).

2. Posiciones

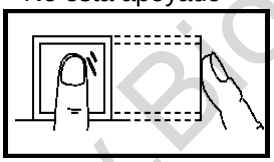
1) Posición del dedo:



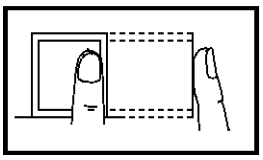
De forma plana, centrado y bien apoyado.

2) Posición incorrecta:

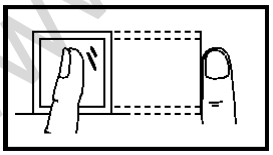
No está apoyado



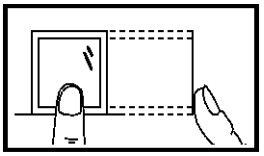
No está centrado



De lado



No está centrado



☺ Nota: por favor asegures que durante el registros de la huella esta sea colocada de una manera correcta de lo contario tendrá problemas a futuro con las Verificación de acceso.

3. LED de Color y su Significado

Trabajando Normal: El Led de color Verde parpadea cada segundo.

Fallo de Verificación: El Led de color rojo encenderá fijamente por un lapso de 3 segundos.

Verificación Completada: El Led de color rojo encenderá fijamente por un lapso de 3 segundos

☺ Nota: Si observa estos leds parpadeando de manera independiente y no cuerda contacte a soporte al cliente.

4. Acerca de este Manual

- Nuestros productos están sujetos a actualización por lo que nuestra empresa no se comprometerá a garantizar la igualdad entre los productos reales y el presente documento, ni asume responsabilidad por cualquier disputa que surja de la discrepancia entre los parámetros técnicos reales y esta manual. Este documento está sujeto a cambio sin previo aviso.
- Las funciones de este manual marcadas con ★ son opcionales lo que quiere decir que no necesariamente las encontrar en el equipo adquirido para adquirir estas funciones contacte a su distribuidor.
- La descripción de imágenes de este manual puede variar ligeramente a la del producto real. Por favor, consulte el producto real para las descripciones exactas.
- La compañía se reserva el derecho de cambio de este documento sin previo aviso.

2. Conceptos Básicos

Esta sección introduce las definiciones de los siguientes conceptos básicos:

- Registro de usuarios
- Verificación de usuarios
- ID de usuario
- Clases de autoridad
- Apariencia del equipo

Las dos funciones más importantes son registro y Verificación de usuarios.

2.1 Registro de Usuarios

El usuario puede registrar arriba de 10 huellas usando el mismo número de ID para tener múltiples selecciones de Verificación. Teóricamente todas las huellas de usuario necesitaran ser registradas por lo que el usuario podrá usar cualquiera para verificar en caso de que este olvide con que huella fue registrado.

Generalmente recomendamos que el usuario registre dos dedos por ejemplo el dedo índice de ambas manos de esta manera podrá seguir verificando sin problemas en caso de suceder un accidente en alguna de sus manos.

2.2 Verificación de Usuario

Cuando el usuario coloque su huella en el lector (1: N) o ingrese la contraseña / colocando la huella después de ingresar el número de ID (1:1), El equipo comparar la huella obtenida con la almacenada. La plantilla de la huella será usada para compararla con el ID. Desde la Verificación el sistema mostrara un comando si esta fue exitosa o no y después será almacenada en el dispositivo.

2.3 ID o PIN de usuario

Cuando se registre una huella el usuario será identificado por su número de ID. Cuando se inicie la Verificación el equipo usara este número de ID para compararlo y verificarlo con la contraseña o huella.

Podrá ingresar el número de ID desde el teclado del equipo, por ejemplo la tarjeta de proximidad (el reconocimiento del equipo debe ser configurado como RF card Reader/lector de tarjetas).

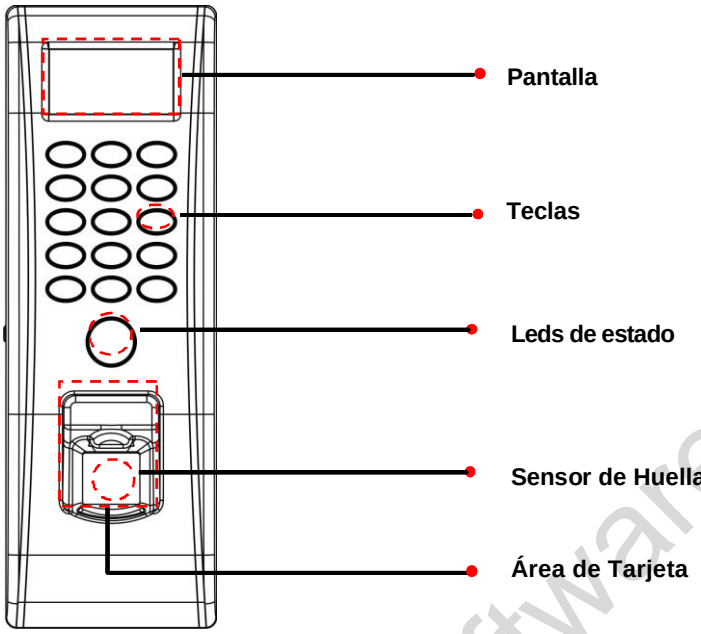
2.4 Clases de autoridad

Los equipos de control de acceso con pantalla blanco y negro contienen dos clases de autoridad:

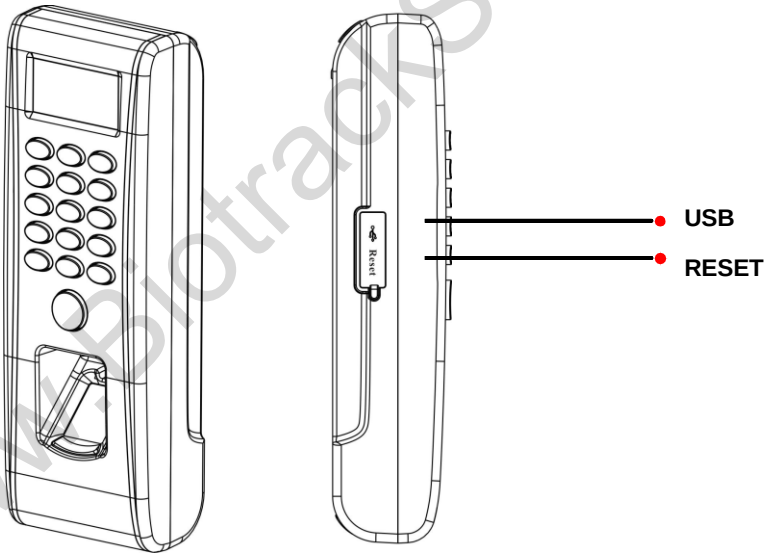
- Usuarios: Se refiere aquellos que necesitan verificar su identidad para un propósito, por ejemplo abrir una puerta o verificar su entrada y salida.
- Administradores: Tienen todos los privilegios sobre los usuarios ordinarios y acceso a todas las funciones y configuraciones del equipo.

2.5 Apariencia del Equipo

Vista Frontal:

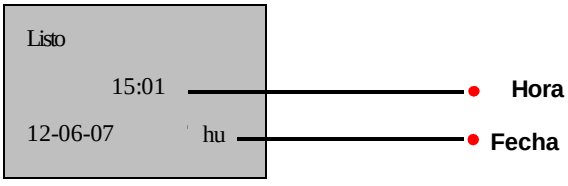


Vista de Lado:



Interfaz inicial:

La primer pantalla mostrada al iniciar el equipo es llamada “Interfaz inicial” como se ve a continuación.



3. Registro y Verificación

A continuación se realizar una introducción de como registrar usuarios en el equipo de control de acceso además de cómo realizar la Verificación:

- ✧ Registro de Usuarios
- ✧ Registro de Copia de Seguridad de Huellas
- ✧ Comandos de Registro Exitoso
- ✧ Verificación de Identidad.
- ✧ Registrar Administrador
- ✧ Borrar Datos de Registro

☺ Nota: Para registrar un nuevo usuario deberá tener los privilegios de administrador.

3.1 Registrar un Usuario

Todos los equipos y lectores de control de acceso con pantalla a blanco y negro soportan tres modos de registro: Registro de huella, contraseña y tarjeta RFID.

Si no existe un administrador registrado entonces cualquier usuario podrá registrar usuarios.

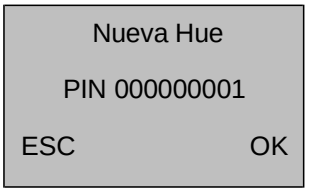
Si ya existe un administrador registrado entonces para registrar un usuario será necesario el primero verificar la identidad del administrador para esto presionamos MENÚ. El sistema pedirá colocar la huella, ingresar la contraseña o pasar la tarjeta del administrador.

☺ Nota:

1. Si necesita borrar los privilegios de administrador haga clic en "Opciones" -- "opciones avanzadas".
2. Tipo de Verificación huella o tarjeta por default para su registro podrá seleccionar el método.
3. Para seguridad recomendamos crear un usuario al iniciar el uso de dispositivo.

3.1.1 Registre una Huella

1) Seleccione **Menú** → **gestión usr** → **grabar usr** para mostrar la interfaz. Seleccione [grabar huella] y presione **OK** para mostrar la interfaz [grabar huella].



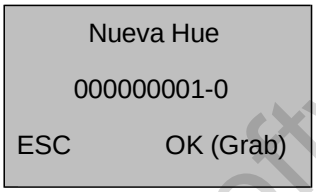
2) ingrese un número (desde 1-999999999) en el [PIN]. Presione **OK** para mostrar la interfaz de registro.

☺ Nota:

El ultimo digito “0” en “000000001-0” muestra la primera huella. “000000001-1” el ultimo digito “1” muestra la segunda huella, significa copia de seguridad de huella.

El equipo muestra 9 dígitos de números y automáticamente agregara 0 como prefijos antes del 9 digito. Por ejemplo i ingresa"11", el equipo mostrara "000000011".

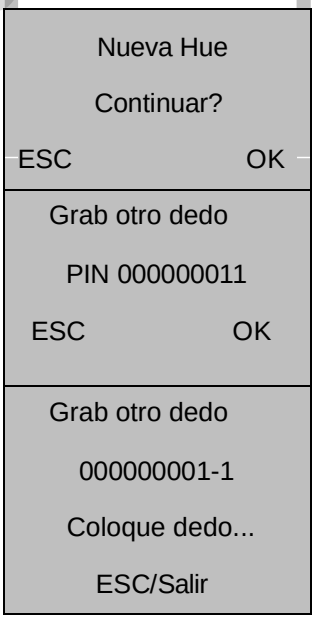
3) Coloque le dedo por tres veces consecutivas de acuerdo al comando emitid por el equipo. Si el registro es completado, se mostrar la siguiente información:



4) Presione **OK** para salvar la huella. Si el registro falla, el sistema le pedirá que reingrese el número de ID y deberá reiniciar el registro desde el paso 2.

3.1.2 Registro de Copia de Seguridad

Si presiona **ESC** en la interfaz [Nueva Huella] cancelar el registro y se mostrar la interfaz [Grabar otro dedo] presione **OK** y se mostrar la siguiente figura:



Los siguientes pasos para registrar una copia de seguridad de una huella son los mismos que al registrar un usuario.

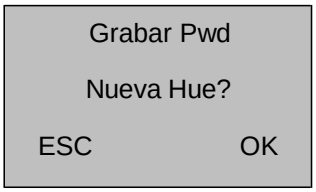
☺ Nota:

Se recomienda el registrar dos huellas por usuario como mínimo.

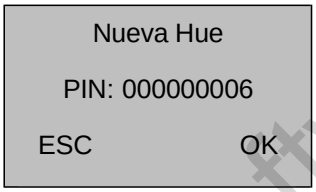
En el registro de copia de seguridad se puede utilizar una huella, contraseña o tarjeta.

3.1.3 Registrar Contraseña

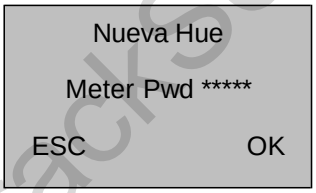
1) Seleccione **Menú** → **gestión usr** → **grabar usr** para mostrar la interfaz [grabar usr] y seleccione [grabar Pwd] y presione **OK** para mostrar la interfaz de registro.



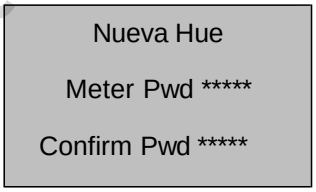
2) Presione **OK** para confirmar.



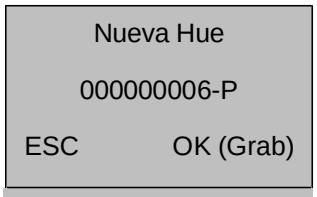
3) Ingrese un número (desde 1–999999999) en el campo [PIN] presione **OK** para mostrar la interfaz de contraseña.



4) Ingrese su password en el campo y presione **OK** para procesar.



5) Re-ingrese su password en el campo [Confirm Pwd] y presione **OK** para confirmar.

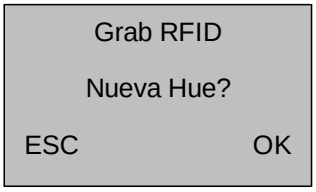


Nota: El último digito "P" en "000000006-P" significa password.

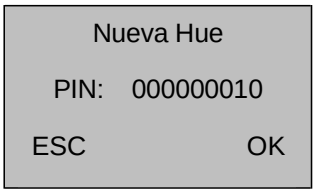
6) Presione **OK** para salvar el dato registrado y salir de la interfaz. Presione **ESC** para entrar a la interfaz de modificación de password los paso serán los mismo que los del registro.

3.1.4 Registrar Tarjeta ID

1) Seleccione **Menú** → **gestión usr** → **grab usr** para entrar a la interfaz. Seleccione [grab RFID] y presione **OK**.



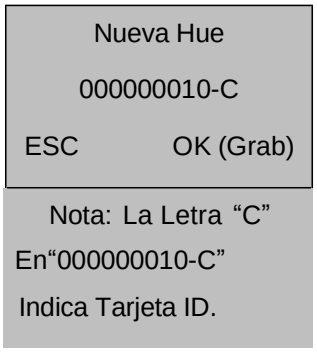
2) Presione **OK** para confirmar.



3) Ingrese u número (desde 1–999999999) en el campo [PIN] y presione **OK** para mostrar la interfaz.

4) Pase su tarjeta por el equipo y el sistema leerá el número.

5) Presione **OK** para confirmar y procesar.



6) Presione **OK** para salvar y completar el registro de la tarjeta. Presione **ESC** para entrar al interfaz de modificación

☺ Nota: Las tarjetas HID y MIFARE son funciones opcionales. Si desea personalizar a estas tarjetas contacte a su representante comercial o ingenieros de soporte.

3.2 Comandos de Registro Exitoso

Una huella registrada con una calidad alta será verificada con una alta velocidad mientras que una registrada con una baja calidad será muy difícil de verificar.

Para mejorar la calidad de las huellas registradas consulte la tabla 3-1

Tabla 3-1 Causas comunes de un mal registro o mala calidad de huella

La huella es muy seca o muy sucia	Frote sus dedos sobre la palma de su mano para que limpie. Sople un poco sobre su dedo para hidratar un poco.
Aplicar insuficiente presión	Aplique una presión ligera y uniforme durante el proceso de registro.
Seleccione dedos a registrar	Se recomiendan los dedos derecho, izquierdo o el de en medio. Seleccione dedos que no estén dañados o tengan cicatrices. Usualmente seleccionan el dedo índice, pero este es de más baja calidad que el dedo de en medio o el dedo del anillo. Para usuarios con dedos pequeños se recomienda usar el dedo gordo. Para registrar huellas de repuesto se pueden seleccionar los dedos no propensos al desgaste natural como el dedo del anillo por ejemplo.
Colocación del dedo	Presione el dedo de manera plana en el sensor y asegúrese que la yema (no la punta) cubra lo más posible del sensor. No lo presione de forma perpendicular en el sensor; no retire rápidamente el dedo del sensor hasta que este lo indique el tiempo estimado de permanencia del dedo en el sensor será de 3 segundos.
Impacto del cambio de imagen de la huella	El cambio de la imagen de la huella dactilar puede suceder por causas accidentales dañando la imagen de la huella y provocando una Verificación fallida. Si persisten las molestias en el uso de una huella por un problema de cambio de imagen de la misma lo recomendable es usar el método de registro y Verificación a través del número de contraseña o password.
Otras Causas	Existen muchas causas por las que un usuario no pasara la Verificación no importa cuántas veces lo intenten si la calidad de la huella es muy mala. En esos casos puede adoptar el modo de Verificación de ID + huella, bajar el rango del umbral 1: 1 o adoptar el modo de Verificación de password.

3.3 Modos de Verificación

Después del registro podrá validar por medio de la Verificación el registro de las huellas, tarjetas o password.

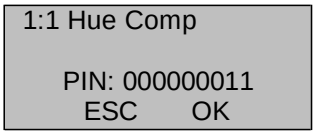
3.3.1 Verificación de Huella

Modo de reconocimiento 1:1 y 1: N para huellas Identificación de huella.

(1) 1:1 Reconocimiento de Huella

En el modo de reconocimiento de huella 1:1, el equipo comparar la huella actual recolectada con el número de ID o PIN ingresado desde el teclado del equipo.

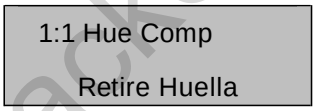
Pasos de operación:



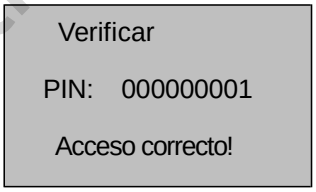
Ingrese el número de ID/PIN en la interfaz principal.

☺ Nota: Si el usuario tiene registrado un password presione **OK** en la Verificación y entrara automáticamente a la interfaz del password. Si no lo tiene entrara a la Verificación de huella.

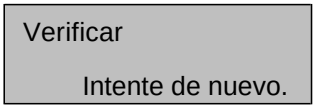
Sugerimos en el uso de la comparación de huellas 1:1 presionar directamente la huella y no presionar **OK**.



Y después coloque directamente su dedo en el lector y le mostrara la siguiente interfaz:



Si la Verificación es completada el sistema genera un comando de voz “Gracias!”.



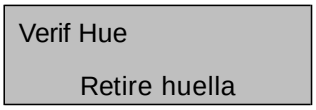
Como se ve en la ventana de arriba aparecerá si la Verificación falla:

Después que la interfaz es mostrad después de 0.5 segundos, el sistema regresara a la interfaz inicial.

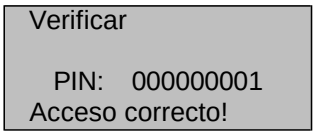
(2) 1: N Reconocimiento de Huella

En el modo de reconocimiento de huella 1: N, El equipo comparar la huella actual recolectad con todas las almacenadas en el equipo.

Pasos de operación:

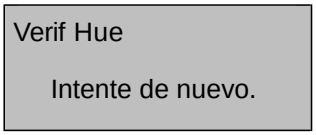


Coloque su dedo en la interfaz inicial y aparecerá lo siguiente:



Si la Verificación es completad el equipo emitirá el comando "Gracias!" después que la interfaz anterior sea mostrada y regresara a la pantalla principal:

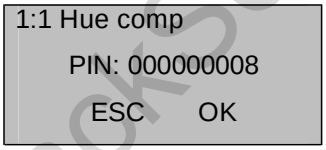
Si la verificación falla, el sistema generara el comando "intente de nuevo!" y mostrar lo siguiente:



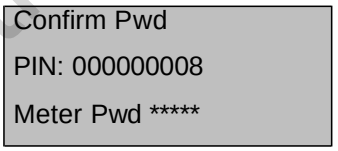
Después de mostrar la interfaz anterior el sistema regresará a la pantalla principal.

3.3.2 Verificación de Contraseña/Password

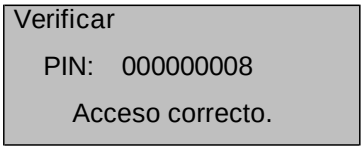
Ingrese su número de ID/PIN en la interfaz inicial.



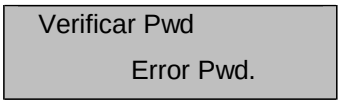
Presione **OK** y aparecerá la siguiente interfaz



Ingrese el correcto password y presione **OK** para confirmar.



En caso de ingresar un password erróneo se mostrara "Error Pwd" y regresar a la interfaz de ingreso de password tendrá solo tres oportunidades de ingreso de password o contraseña



3.3.3 Verificación con Tarjeta de Proximidad★

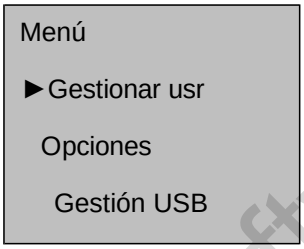
Si tiene un número de tarjeta ID registrado en el sistema podrá realizar una Verificación de tarjeta solo pasando la misma por el área correcta del equipo.

3.4 Registro de Administrador

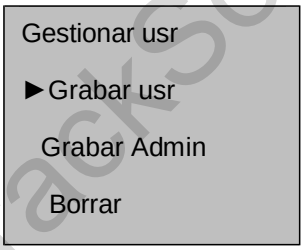
Los equipos y lectores de control de acceso le brindan la configuración de un administrador para prevenir cambios de datos no autorizados en el sistema brindando una mayor seguridad. Las configuraciones para la creación de un administrador son las siguientes:

1) Por default de fábrica obtendrá el equipo sin ningún administrador solo presione **Menú** para accesar al sistema.

La siguiente interfaz será mostrada.

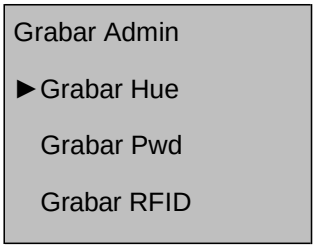


2) Presione **OK** para mostrar la interfaz de Gestionar usr.



3) Seleccione **Grabar Admin** con la teclas ▲/▼.

4) Presione **OK** para ver la interfaz.

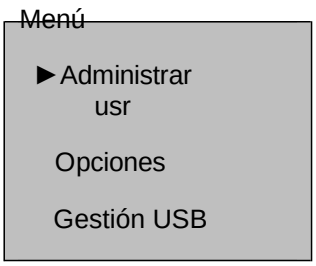


5) Seleccione el modo de registro y presione **OK** para mostrar la interfaz de registro. Después los siguientes paso serán mismos como al registrar un usuario. Para detalles vea 3.1.1Registro de Usuario.

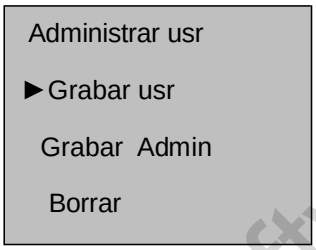
3.5 Borrar Datos de Registro

Para borrar usuarios registrados en el sistema deberá realizar lo siguiente:

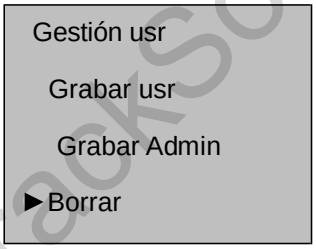
1) Presione **Menú** para entrar al menú principal:



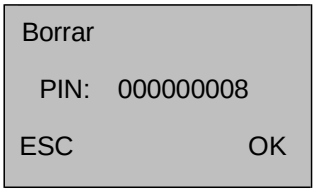
2) Presione **OK** para entrar a la interfaz.



3) Seleccione **Borrar** usando las teclas ▲/▼.



4) Presione **OK** para mostrar la interfaz de borrar.

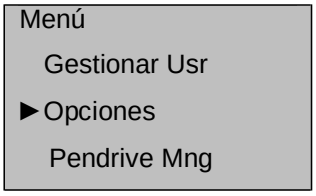


5) Ingrese un número en el campo [PIN] y presione **OK** para confirmar. Después se borrara el usuario seleccionado con un comando de confirmación.

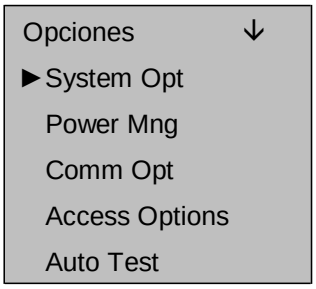
☺ Nota: Para borrar los privilegios de administrador o todos los datos puede escoger “Menú”-- “Opciones” -- “Opc sist” -- “opc avanz”-- “bor.priv.admin” o “borrar datos”.

4. Configuraciones

Presione **Menú** después de verificar el administrador e ingrese al menú del equipo.



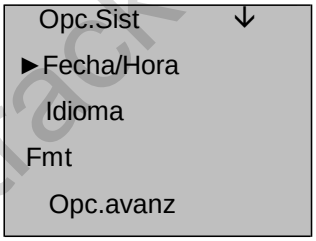
Seleccione **Opciones** y presione **OK**.



El menú de **Opciones** contiene 5 submenús: **Opc.Sist**, **Gest.Alim**, **Comm.Opc, Opc acceso** y **Auto Test**. Estos serán descritos en las siguientes partes.

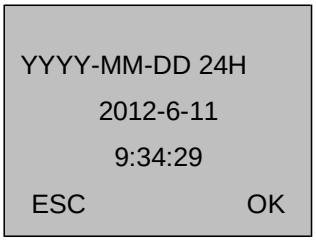
4.1 Configuración del Sistema

Seleccione **Opc.Sist** y la información será mostrada como a continuación:



4.1.1 Fecha/Hora

Configure la fecha y hora actual que será mostrad en el equipo. Presione **OK** para entrar a la interfaz.

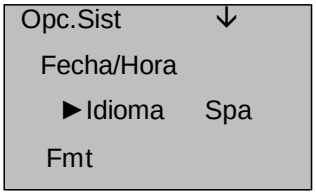


Para modificar deberá usar la teclas ▲/▼ t configurar la fecha y hora deseada después presione **OK** para salvar.

☺ Nota: En algunos equipos deberá presionar la tecla de MENÚ por 3 segundos para confirmar.

4.1.2 Idioma★

Seleccione el lenguaje deseado escoja **Lenguaje** y presione **OK** para mostrar la interfaz de edición. Si selecciona **English**, la información en la pantalla será mostrada en inglés.



Puede cambiar los tipos de lenguaje usando la teclas ▲/▼ seleccione le lenguaje deseado y presione **OK**. Después presione **ESC** para salir de la interfaz. Cuando aparezca el comando de confirmación para salvar presione **OK**. Después deberá reiniciar el equipo para que lo cambios tomen efecto.

☺ Nota: La selección del lenguaje no es una función estándar. Si necesita agregar esta función por favor contacte al departamento de ingeniería de soporte.

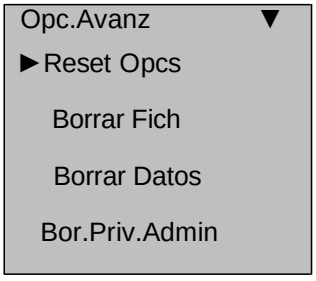
4.1.3 Formato de Fecha (FMT)

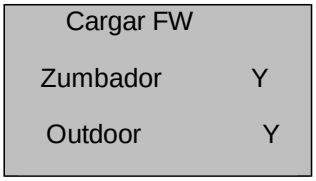
Podrá seleccionar el formato deseado a visualizar en la pantalla seleccione **Fmt** y presione **OK** para mostrar la interfaz. Seleccione el deseado con las teclas ▲/▼ actualmente el sistema soporta 10 formatos de fecha: YY-MM-DD, YY/MM/DD, YY.MM.DD, MM-DD-YY, MM/DD/YY, MM.DD.YY, DD-MM-YY, DD/MM/YY, DD.MM.YY y YYYYMMDD. Seleccione el deseado y presione **OK** para confirmar después presione **ESC** para salir de la interfaz. Cuando el equipo le pida una confirmación presione **OK** y el formato de fecha será modificado.

Por ejemplo el formato de fecha **MM/DD/YY** y **YY-MM-DD** son mostrados en la figura abajo

4.1.4 Configuraciones Avanzadas (Opc.Avanz)

Desde esta opción podrá realizar varias operaciones como resetear a valores de fábrica, borrar registros de asistencia, borrar todo dato, borrar privilegios de administrador, actualizar firmware, sonidos, como se muestra a continuación:





☺ Nota: las opciones mostradas en el menú de arriba algunas son opcionales. Si el producto con el que cuenta no tiene algunas de estas es porque no las soporta(s).

Seleccione la opción deseada usando las teclas ▲/▼.

1) Reset Opcs

Esta opción regresará el equipo a valores de fábrica.

2) Borrar Fich

Borrara todos los registros de transacciones y eventos.

3) Borrar Datos

Borrar todas las huellas y registros del equipo.

4) Bor.Priv.Admin

Cambiarán todos los administradores a usuarios ordinarios.

5) Cargar FW

Puede usar esta opción para actualizar el firmware del equipo desde una memoria USB.

☺ Nota: Si necesita un firmware para actualizar, por favor contacte a departamento de ingeniería de soporte de su localidad generalmente no recomendamos actualizar el firmware.

6) Zumbador

Activara el sonido seleccionando “Y” esto se escuchara al presionar los botones del equipo para silenciar estos sonidos seleccione “N”.

7) Modo fuera de Puerta

En este modo si selecciona “Y” la pantalla mostrara títulos en blanco en la parte trasera del display después de reiniciar el equipo.
Si selecciona “N” y la pantalla aun muestra estos títulos reinicie le equipo.

4.2 Administrar Alimentación★

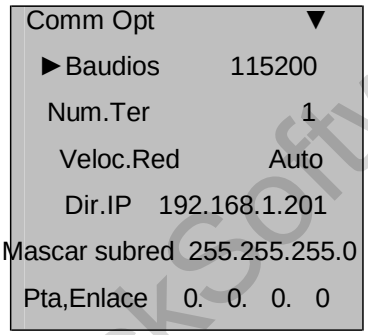
Presione **Menú** seleccione **Opciones** → **Gest.Alim** para ver la interfaz:

Min Reposo

Existen dos opciones asociadas cuando se configura a 0, estará deshabilitada. Por ejemplo si se configura a 1, es equipo entrara a un estado de reposo al no ser manipulado después de un minuto.

4.3 Configuraciones de Comunicación

Presione **Menú** seleccione **Opciones** → **Comm. Opc** para ver la interfaz:



1. Baudios

Esta opción es usad para configurar el rato de baudios en la comunicación entre el equipo y la PC. Contienen 5 opciones: 9600, 19200, 38400, 57600, y 115200. El rato más alto es recomendado para la comunicación RS232 obteniendo una alta velocidad, para establecer la comunicación RS485 el rato más bajo será recomendado.

2. Num.Ter

Esta opción refiere al número de ID del equipo puedes ser configurado desde 1 a 255.

3. Velocidad de Red

Este parámetro refiere al rato de la red, contiene 5 opciones: AUTO, 10M-H, 100M-H, 10M-F y 100M-F.

4. Dirección IP

Esta por default será 192.168.1.201. Pero podrá modificarlo si lo desea.

5. Mascara de Subred

Por default este será 255.255.255.0. Pero podrá modificarlo si es necesario.

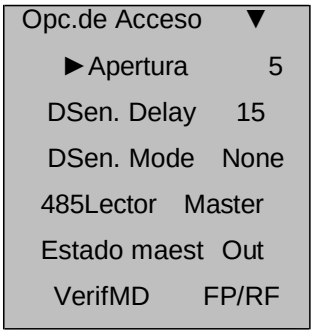
6. Puerta de Enlace

Esta por default será 0.0.0.0. Pero podrá modificarla si lo desea.

4.4 Opciones de Acceso★

Los equipos y lectores de control de acceso de esta línea funcionan de la mano con el software de control de acceso *Access3.5* as standard como funciones estándar las funciones incluyen Zonas de tiempo de acceso, días festivos, vinculaciones, Anti-passback, First-card, Multi- etc., pero no las funciones de Interlock. Para detalles de las operaciones refiérase al manual de usuario del software

Presione **Menú** seleccione **Opciones** → **Opc.de Acceso** para ver la interfaz
Como se muestra a continuación:



4.4.1 Apertura

El tiempo de duración de una chapa electrónica después

Para configurar realice lo siguiente: Seleccione apertura y presione OK. Después ingrese el número designado de segundos y presione ESC para salir y salvar.

“S (segundos)” para seleccionar la duración podrá configurar desde 1~10s (en algunos casos se puede configurar hasta 254s).

Si se configura a“0”significa que la duración estar cerrada. Por lo que no se recomienda dejar en“0”.

4.4.2 DSen. Delay

Retardo del sensor de puerta. Una alarma será generada al sobre al sobre pasar este periodo de tiempo and este periodo será llamado Door sensor delay.

4.4.3 DSen. Mode

El sensor de puerta incluye tres modos: NONE/ninguno, Normalmente abierto (NO), y

normalmente cerrado (NC). “NONE” o ninguno se usara si no hay sensor conectado.

“NO”: puerta y chapa estarán abiertas; de lo contrario se generara la alarma. “NC”: puerta y chapa

estarán cerrados ; de otra manera la alarma será generada.

4.4.4 485Lector★

Presione **Menú** seleccione **Opciones** → **Opc de Acceso**→ **485Lector** como se muestra:

Access Options	▼
Apertura	5
DSen. Delay	15
DSen. Mode	None
► 485RLector	Master
Estado maest	Out
VerifMD	FP/RF

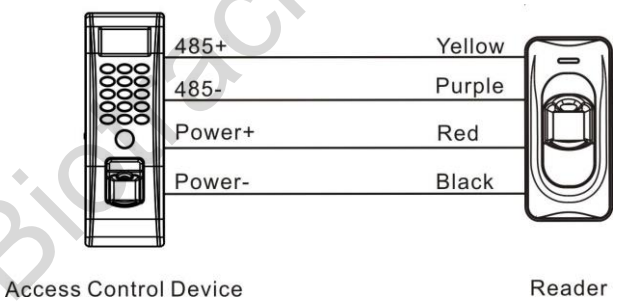
El equipo soporta la función de lector 485 y mediante esta puede ser conectado a un lector FR1200.

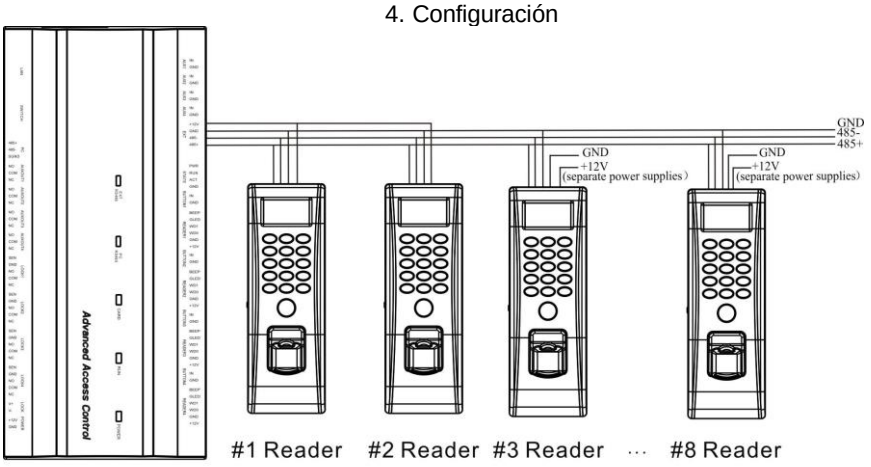
Mientras tanto puede actuar como un esclavo/maestro a un control de acceso como esclavo ya un FR1200 como maestro y usar las funciones de antipassback.

Si selecciona “Maestro”, la función será abierta y el equipo funcionara como un controlador si selecciona “Esclavo” el equipo actuara como un lector si selecciona “No”, la función será cerrada y el equipo podrá ser conectado a una PC mediante la comunicación RS485

☺ Nota: El equipo actuara como maestro esclavo si esta función es abierta entonces el equipo no podrá conectarse por RS485 a la PC deberá cerrar la opción y reiniciar el equipo para que los efectos tomen efecto

.





inBIO Controller

Note: Set the RS485 address(device number) by Access3. 5 software.

4.4.5 Estado maestro ★

Este estado contiene dos tipos: Entrada o Salida.

Configure el estado maestro o como “Salida” e instale dentro de la puerta el esclavo como "Entrada" e instálelo fuera de la puerta. Los registros de entrada y salida serna almacenados en el equipo maestro.

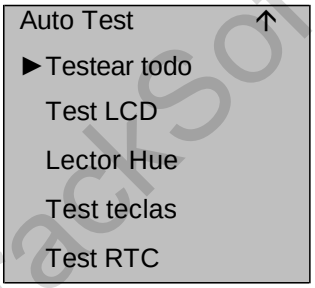
4.4.6 VerifMD

El equipo soporta varios modos de verificación como huella o tarjeta ID (FP/RF), huella más tarjeta ID (FP&RF), Password mas tarjeta ID (PW&RF), huella, Password (PW), tarjeta (RF).el modo de verificación por default del equipo será huella o tarjeta (FP/RF).

Si necesita cambiar el modo de verificación puede entra al modo de verificación para cambiarlo. La ruta será: MENÚ →Opciones → Opc.de Acceso→ VerifMD.

4.5 Auto test

Seleccione **Auto Test** para entrar a la interfaz siguiente:



Desde esta operación podrá probar todos los componentes. Esta opción ayuda a encontrar y solucionar la mala función de un componente fácil y rápido.

Test LCD: El equipo automáticamente probara los efectos de la pantalla LCD con imágenes.

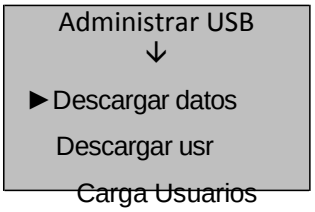
Lector de Hue: Se realizara una prueba del funcionamiento correcto del sensor de huellas. Después de seleccionar presione "OK” para iniciar la prueba al terminar presione" ESC "para salir.

Test Teclas: Se realizara una prueba de cada uno de los botones del teclado. Presione cualquier tecla del teclado del equipo y esta será mostrada en la pantalla. Presione “ESC” para salir.

Test RTC. Se realizar la prueba correcta del paro del reloj para asegurar el funcionamiento de este inicie presionando "OK" para la prueba al terminar presione "ESC" para salir.

5. Administración de USB ★

Seleccione **Administrar USB** y aparecerá la siguiente interfaz:



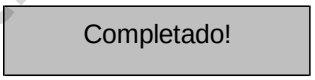
Y Podrá descargar los datos de asistencia, datos de empleados, mensajes cortos y también cargar la misma información desde una memoria USB.

5.1 Descarga Datos de Asistencia

1. Inserte la USB a la interfaz del equipo.

2. Seleccione **gestión USB** y seleccione la opción deseada usando las teclas "▲/▼" la interfaz ser amostrada como a continuación:

3. Presione **OK** para confirmar e iniciar la descarga. Una vez completad la operación la interfaz mostrada será la siguiente:

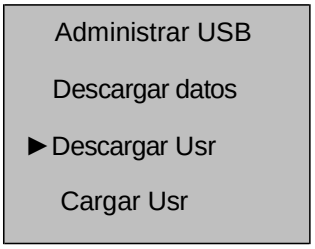


4. Presione **ESC** para regresar a la interfaz inicial y remueva la USB. El archivo con los datos será **attlog.dat** .

☺ Nota: Una vez completada la descarga el equipo emitirá un comando de confirmación de lo contario si este pregunta por el USB deberá revisar que este se encuentre conectado de manera correcta.

5.2 Descargar Datos de Usuario

La descarga de los datos de usuario es la misma que la de las transacciones seleccione con ▲/▼ la opción "Descarga usr" desde el menú de la interfaz.

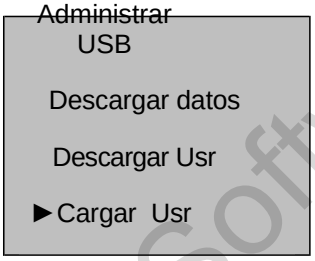


Los archivos user.dat (información de usuario), userauth.dat (privilegios de usuario) y timezone.dat (periodos de tiempo) serán los descargados al disco USB. Tres archivos al mismo tiempo.

☺ Nota: Si el equipo contienen otras funciones diferentes en la descarga de las huellas el archivo será nombrado como "template.fp10".

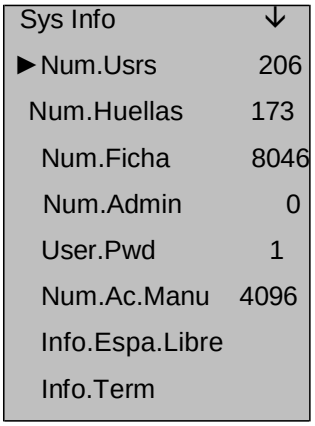
5.3 Cargar Usuarios

Presione ▲/▼ para seleccionar “Cargar usr” desde “Administrar USB” y presione **OK**. Los archivos user.dat (información de usuario), userauth.dat (privilegio de usuario) y timezone.dat (zonas de tiempo) guardados en la USB serán cargados al equipo.



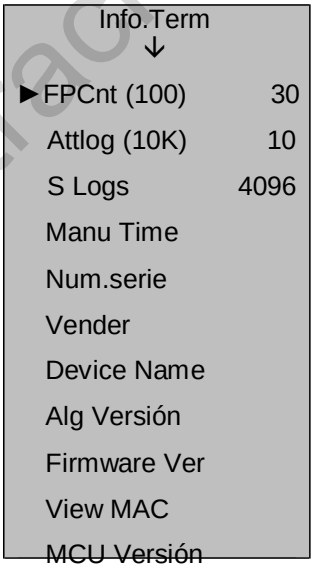
6. Información del Sistema

Desde la opción **Inf.Sist** podrá revisar la información del equipo como la cantidad de huellas registradas, usuarios registrados, registros de asistencia, administradores registrados e información del equipo. Desde el **Menú** seleccione **Inf, Sist** presione **OK** para ver la interfaz siguiente:



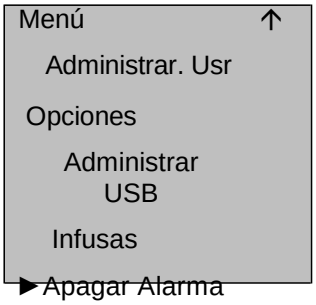
Como se muestra en la figura de arriba podrá revisar **Num.usrs** (número de usuarios registrados), **Num.Huellas** (número de huellas registradas), **Num.Ficha** (Registros de asistencia), **Num.Admin** (número de administradores registrados), **User.Pwd** (Número de password) y **Num.Ac.Manu** (número de accesos al menú). En la opción **Info.Espa.LIbre** podrá ver el espacio de almacenamiento libre del equipo.

Desde **Info.Term** podrá ver la información como capacidad de almacenaje, fecha de creación, número de serie, fabricante, versión de algoritmo y versión de firmware.



7. Apagar Alarma ★

La opción **Apagar Alarma** solo después de que el equipo genera la alarma y se usara para resetearla. Desde el **Menú** seleccione **Apagar Alarma**.



☺ Nota: Esta opción solo aparecerá después que se genere la alarma.

8. Mantenimiento

1. Limpieza

Algunas veces los lentes ópticos, teclados y pantallas necesitaran ser limpiados. Aunque el ciclo de limpieza específica depende del entorno ambiental en que opera el dispositivo, la siguiente guía de mantenimiento podría ser de alguna ayuda:

Tabla 1-1 descripción de mantenimiento

Ítem	Limpieza
Teclado y Pantalla	Limpie estos cuando la superficie esté demasiado sucia o la pantalla esté borrosa.
Lentes ópticos	No los limpie frecuentemente. Los lentes ópticos trabajan mejor con aceite o grasa.
	Limpie si estos están borrosos y afecta la verificación de los usuarios.

2. Limpiar Teclados y Pantallas LCD

Antes de limpiarlos apague por completo el equipo, límpielos con un paño húmedo o detergente neutral y después seque con un paño seco.

3. Limpiar Lentes Ópticos

Siga las siguientes sugerencias para limpiar estos lentos después de apagar el equipo:

1) Sople el polvo o suciedad de la superficie de estos.

2) Limpie la pantalla con cinta adhesiva.

Precaución: No limpie los lentes ópticos con agua o detergente no-neutral; de lo contrario el lente se dañara de manera permanente.

3) Limpie el lente con un paño de micro fibra fina teniendo cuidado de no rayarlo. Existen paños especiales para la limpieza de los lentes ópticos.

9. FAQs

1. Pregunta: Como soluciono el problema de algunos usuarios que no pueden verificar con su huella pero otros no tienen problemas?

Respuesta: Los siguientes factores pueden causar una verificación difícil en los usuarios:

①. Las huellas dactilares de algunos usuarios están desgastadas.

②. Los dedos tienen demasiadas arrugas que cambian con frecuencia.

❍ La piel del dedo está en mal estado.

Para usuarios con este problema pueden borrar esa huella y registrarlos con otra huella.

Se recomienda usar dedos con buena calidad (sin arrugas, sin cicatrices) para el registro. Presione el dedo de manera palma en el sensor y asegúrese de que la yema del dedo (no la punta) cubra lo más posible el sensor. Al terminar con el registro de un usuario se recomienda probar la verificación, recuerde que puede registrar más huellas por usuario.

Además el equipo ofrece el modo de reconocimiento 1:1 y verificación de password o contraseña especialmente para los usuarios a quienes le s es difícil realizar la verificación mediante la huella.

2. Pregunta: Cuales son las causa comunes de la falla de comunicación del equipo?

Respuesta: A continuación se enlistan las posibles causas:

① La configuración del puerto de comunicación es incorrecta. El puerto de comunicación configurado no es el usado actualmente.

② La configuración del rato de baudios de la comunicación de la PC no es consistente con la del equipo.

❍ El equipo no está conectado a la fuente de alimentación o con la PC.

④ El equipo está conectado con la PC pero no está alimentado.

⑪ El número de la terminal conectada es incorrecto.

⑥ El cable de datos o el convertidor está dañado.

⑦ Falla en el puerto COM de la PC.

3. Preguntas: Cual es la causa de una pantalla media (algunas veces media pantalla) o borrosa después de encenderlo? Como arreglarlo?

Respuesta: A continuación se enlistan las posibles causas:

① La mainboard está dañada.

② La pantalla LCD está dañada.

En cualquiera de los dos caso deberá contactara su distribuidor para realizar la reparación respondiente.

4. Pregunta: Como puedo Borrar un Administrador?

Respuesta: Presione **Menú--Opciones--Opc.Sist -- Opc.Avanz-- Bor.Adm.Priv**.

De otra manera conecte el equipo a la PC estableciendo una comunicación. Seleccione la opción de administración de equipo y haga clic en **Borrar administrador** para esta función de esta menar podrá entrar al menú después de realizar esta operación y desconectar el equipo de la PC.

5. Pregunta: Porque se escucha un beep durante la comunicación entre el equipo y la PC?

Respuesta:

① Si este beep ocurre en el modo de comunicación RS-232 la configuración del rato de baudios de la PC y el equipo es inconsistente.

② Si este beep ocurre en el modo de comunicación RS-485 es porque los cables del convertidor están invertidos están haciendo contacto uno con otro.

6. Pregunta: Porque el equipo muestra constantemente "por favor presione (remueva) su dedo nuevamente" sin que este alguien cerca? Como arreglarlo?

Respuesta: Las posibles causas son las siguientes:

① Hay suciedad, grasa o una ralladura en la superficie del sensor lo que hace que el sensor presienta la detección de una persona constantemente. Remueva la suciedad o grasa del sensor con una cinta adhesiva

② El cable del sensor de huellas se ha dañado o esta desconectado.

❍ El chip de la mainboard está dañado.

En los últimos dos casos le sugerimos contactar a su distribuidor para reparaciones.

7. Pregunta: Porque hay una falla o produce un error cuando leo los datos de asistencia aunque puedo descargar los datos de huellas y contraseñas correctamente? Cómo arreglarlo?

Respuesta: Este problema se relaciona al cable de datos, convertidor o configuración del puerto COM de la PC. Intente disminuir el rato de baudios de la PC y el equipo, por ejemplo configúrelo a 19200 o 9600 antes de intentar de nuevo.

10. Apéndice

Las funciones descritas en el apéndice son opcionales. Si necesita estas funciones por favor contacte a su representante comercial o al departamento de ingeniería de soporte.

10.1 USB

USB Host

El equipo es usado como USB Host y es conectado con un disco USB para cambio de datos.

Los lectores de huella convencionales transfieren datos solo mediante RS232, RS485 o Ethernet. Por lo que esta transmisión de datos puede alargarse por un largo periodo de tiempo. La opción USB supera la velocidad de transferencia de datos de los modos anteriores. Inserte el USB a la ranura del equipo descargue los datos a este y después conéctelo a su computadora para importar los datos. También se puede usar esta función de USB para transmitir los datos de usuario o usuarios de un equipo a otro sin tener que conectar los dispositivos al PC con cables de red.

USB Cliente

Conecte el equipo con la PC y transfiera los datos guardados en el equipo a la PC mediante el cable USB.

Cuando el equipo es usado como USB Cliente Las opciones para configurar la comunicación USB serán mostradas en el menú de configuración de comunicación del equipo.

Nota: Cuando el equipo se conecte a la CC como USB Cliente la PC deberá tener instalado el driver actualizado.

10.2 Timbre

La mayoría de las compañías usan un timbre para iniciar y finalizar los turnos por lo regular una manual o un eléctrico. Para ahorrar costos y facilitar la administración hemos integrado esta función a nuestros equipos. La opción de **Timbre** está disponible en los equipos que soporten dicha función. Existen 8 segmentos de tiempo disponibles para cada día de la semana los cuales podrá configurar a sus necesidades. El equipo automáticamente activara el timbre a la hora configurada.

El equipo activara el timbre de las siguientes dos maneras:

Activar el timbre desde la bocina instalada en el equipo.

Conectar una eléctrica al equipo. El equipo activara este timbre mediante una señal de relé.

10.3 Conexión Externa con un Lector de Huellas

Esta función es especialmente para equipos configurados con una interfaz USB. Inserte el lector de huellas en el puerto USB, Seleccione lector de huellas desde **Menú → Opciones → Opc.Avanz → Conectar con lector FP** y configure la opción **Conectar con Lector FP** a **Y**. Después de eso el lector de huellas externo y el sensor de huellas del equipo podrán ser usados.

Cuando se use para tiempo y asistencia, el lector externo podrá ayudar a desviar parte de los usuarios; al usar con control de acceso, el lector puede instalarse en la parte exterior de la puerta mientras que el equipo en la parte interior.

☺ Notas:

1) Después de conectado el lector de huellas exterior el equipo deberá ser reiniciado.

2) Solo los lectores de huellas con licencia SDK podrán ser usados para conexiones externas.

10.4 Modem

[Vista]

To para habilitar la conexión remota entre el equipo y la PC en áreas donde el acceso de internet no está disponible algunos equipos soportan el protocolo de conexión Point-to-Point (punto a punto) (PPP). Esta conexión es un tipo de conexión de end-to-end (final a final) sobre cables telefónicos. La PC implementara un acceso a la red dial-up mediante un Modem. El equipo deberá estar conectado al Modem el cual está conectado mediante un cable telefónico PSTN. El equipo accesará a la red exitosamente mediante dial-up

10.5 Función GPRS

Llamado por sus siglas en ingles General Packet Radio Service (GPRS) es un servicio portador de paquetes de datos desarrollado en base de la comunicación del sistema global de móviles (GSM). Como un paquete de sistema de conmutación, El GPRS es especialmente adecuado para la transmisión de paquetes de datos intermitentes, esporádicos, frecuentes o pequeños. Esta característica es ideal para la mayoría de aplicaciones móviles, por ejemplo la oficina móvil y acceso a internet. El GPRS demuestra capacidades sobresalientes en términos de velocidad de transmisión, gestión de recursos de radio y facturación.

Nuestro equipos son compatibles con la función GPRS ya sea incorporada o externa para implementar la transmisión de datos a través de estepa más detalles de esta operación vea el instructivo del mismo.

10.6 Función WIFI

Wireless Fidelity (Wi-Fi) también conocida como 802. 11b standard. La gran ventaja del Wi-Fi es la alta transmisión de más de 11Mbps. Wi-Fi también tiene una larga distancia de conectividad y una gran compatibilidad con varios de los ya existentes equipos 802.11 DSSS. IEEE 802.11b es una variante basad en radio de IEEE 802.11. El ancho de banda de IEEE 802.11b puede estar arriba de 11 Mbps y ajustarse automáticamente a 5.5Mbps, 2Mbps y 1Mbps dependiendo la fuerza de la señal ay el nivel de interferencia asegurando así la estabilidad y confiabilidad de la red. Principales ventajas: Alta velocidad de transferencia y fiabilidad. La distancia de la comunicación puede ser de hasta 305 m en un área abierta y 76 m hasta 122 m en un área cerrada. La señal Wi-Fi puede ser convenientemente integrada con la red Ethernet alámbrica existente minimizando el costo de redes.

Nuestros dispositivos son también compatibles con el módulo de WIFI ya sea incorporado o externo para implementar la transmisión de datos inalámbrica a través de esta conexión.

Para detalles de operación vea el manual de usuario relación de esta función.

10.7 Consulta de Asistencia

Podrá consultar los datos de asistencia de individualmente de un empleado o de todos los empleados directamente en el equipo si este soporta la función de consulta de datos de asistencia. Esto ayuda a eliminar la molestia de instalar el software y conectar el dispositivo para la descarga de asistencia y consulta facilitando de igual manera a los empleados a consultar sus propios datos de asistencia.

10.10 Mensajes Cortos

Algunos modelos de equipos soportan la transferencia de mensajes públicos y privados en tiempo específico y para una persona en específico. Puede crear estos mensajes en el software y cargarlos al equipo. Los mensajes cortos serán mostrados en la pantalla durante todo el tiempo que el equipo permanezca encendido, mientras que lo privados solo después de la verificación. Esta función ayuda a reducir el trabajo para recursos humanos e incrementa la eficiencia de comunicación.

Un mensaje corto solo para una persona: Si el cumpleaños de un empleado es en Octubre 20, podrá crear un mensaje que diga “Feliz cumpleaños!” desde el software y cargarlo al equipo y configurarlo para sea mostrado en Octubre 20. El mensaje aparecerá en la pantalla después de que el empleado verifique su acceso.

Un mensaje corto para un grupo de empleados: Por ejemplo una junta programada para junio 19 podrá crear un mensaje corto “Por favor asistir a la junta del día ×× en el ×× salón” (podrá editarlo si lo requiere) y desde el software cargarlo al equipo. Y en junio 19, este mensaje será mostrado en la pantalla para la visualización del grupo de personas.

Configurando un mensaje corto: después de configurar un mensaje corto en el software, cárguelo al equipo. El equipo soporta la importación de mensajes en dos modos.

- Directamente del software al equipo.
- Importándolos desde una memoria USB.

Descripción de operaciones:

1. Cree un mensaje corto con el **software externo**→ **SMS Mng** y conecte el equipo a la POC para cargar el mensaje.

2. Cree un mensaje corto con el **software externo**→ **SMS Mng** después cárguelo a → **disco USB**→. Inserta inserte el USB al equipo y cárguelo **Menú** → **Pendrive Mng** → **cargar SMS** para cargar el mensaje desde su USB al equipo.

Recuerde que los mensajes públicos serán mostrados en la pantalla desde que el equipo sea encendido mientras que los mensajes privados solo se mostraran al usuario después de su verificación.

☺ Nota: Podrá cargar como máximo 1024 mensajes al equipo incluyendo ambos privados o públicos.

10.11 Modos de Múltiple verificación

Actualmente el dispositivo está a la altura de los requisitos de acceso con el modo de verificación de solo huella, password e ID + huella. Para proporcionar un sistema de control de acceso La mayoría de nuestros equipos soportan la personalización para la opción de multi verificación de esta manera brindando una mayor seguridad de verificación. Aparte de solo huella, solo password e ID + huella, los equipos soportan los modos de ID (PIN), huella (FP), password (PW) y RF.