



CERRADURA DE HUELLA DIGITAL, NIP Y LLAVE

SKU:BLUE -92



(81) 83155764



ventas@bluemetric.mx

Manual de usuario de bloqueo de huellas dactilares

Versión: 1.0

Fecha: abril de 2010

Acerca de este manual

Este manual presenta la interfaz de bloqueo de huellas dactilares y las operaciones del menú. Para el instalación de bloqueo de huellas dactilares, consulte las instrucciones de instalación animadas.



Nuestros productos están sujetos a actualizaciones de vez en cuando, por lo que nuestro empresa tampoco se comprometerá a garantizar la coherencia entre los productos reales y este documento, ni asumir ninguna responsabilidad por cualquier disputa que surja de la discrepancia entre los parámetros técnicos reales y este manual. Este documento está sujeto a cambios sin previo aviso.

Tabla de contenido

1 Instrucciones de uso.....	1
1.1 Introducción a las funciones de bloqueo de huellas dactilares.....	1
1.2 Lista de accesorios de instalación.....	2
1.3 Requisitos de instalación.....	4
1.4 Vistas delantera y trasera.....	7
1.5 Precauciones.....	10
1.6 Privilegios de usuario.....	11
1.7 Establecer hora.....	11
2. Inscripción y Verificación.....	13
2.1 Registrar un administrador.....	13
2.1.1 Registrar una huella digital.....	14
2.1.2 Registrar una contraseña.....	15
2.1.3 Registrar una tarjeta ID RF.....	dieciséis
2.2 Registrar un Usuario Ordinario.....	18
2.3 Inscripción de respaldo.....	20
2.4 Establecer verificación de usuario y estado NO.....	21
2.5 Gestión de tarjetas FP *	22
2.5.1 Crear una tarjeta PIN.....	23
2.5.2 Registrar una Tarjeta FP.....	25
2.5.3 Crear una tarjeta FP.....	27
2.5.4 Purgar una tarjeta FP.....	28
2.6 Eliminar datos de usuario.....	29
3. Información y configuración de la función de bloqueo.....	32
3.1 Ajustes de funcionamiento.....	32

»

3.2 Ajustes de idioma.....	34
3.3 Contraseña de la tarjeta FP.....	35
3.4 Configuración avanzada.....	35
3.5 Examinar información del sistema	36
3.6 Examinar registros.....	37
3.7 Gestión de memorias USB.....	38
4. Convenciones sobre otras funciones.....	41
4.1 Indicaciones de operación de rutina.....	41
4.2 Prevención de pérdidas del administrador.....	41
4.3 Protección de bajo voltaje de la batería.....	41
4.4 Salida automática del programa y apagado del sistema.....	42
4.5 Descripción del uso de energía externa.....	42
4.6 Desbloqueo con Llave Mecánica de Emergencia.....	43
Apéndice.....	45
Especificaciones técnicas.....	45

1 Instrucciones de uso

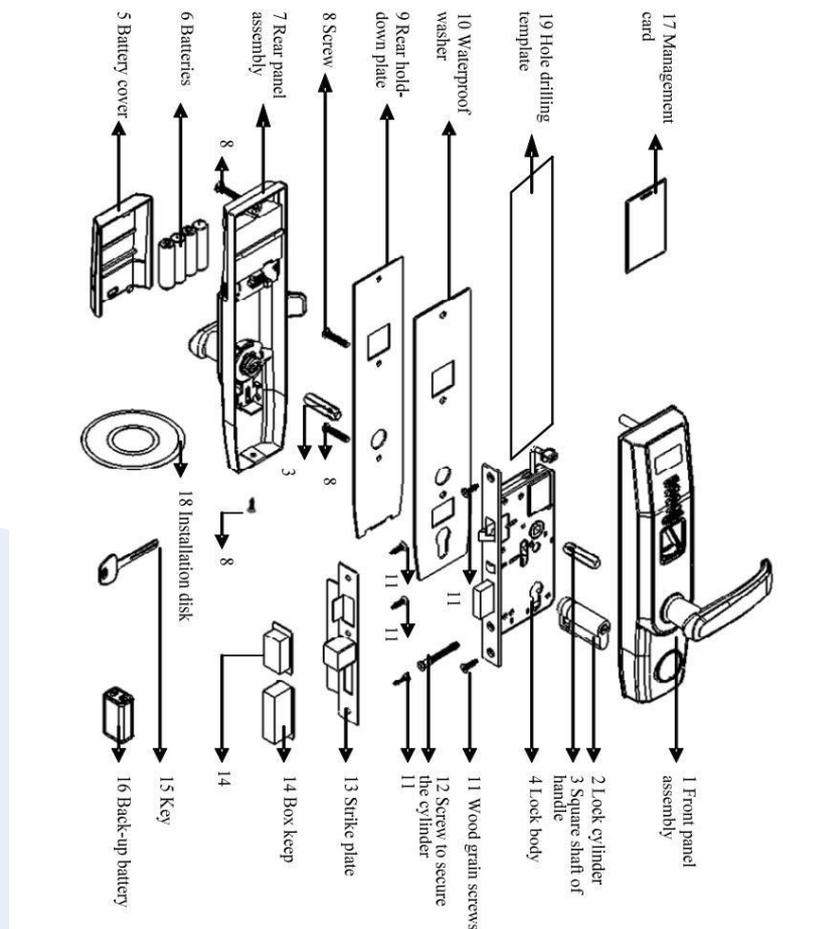
Las funciones marcadas con “y” en este manual solo son compatibles con un producto específico o un producto hecho a medida y se describen a continuación.

1.1 Introducción a las funciones de bloqueo de huellas dactilares

1. Al aprovechar la combinación perfecta de biometría y criptografía, nuestro
los bloqueos de huellas dactilares garantizan una doble seguridad a través de la
huella dactilar + contraseña función de desbloqueo.
2. La pantalla LED orgánica (OLED) de última generación ofrece lecturas nítidas y brillantes
y hace que nuestros bloqueos de huellas dactilares sean intuitivos y fáciles de usar.
Simplemente puede usar
nuestra huella dactilar se bloquea con facilidad después de seguir las instrucciones de
operación para
una vez.
3. Configuración de soporte de privilegios clasificados para superadministradores, administradores
y usuarios ordinarios.
4. Admite la eliminación de todos o los datos de registro especificados.
5. Admite actualización de firmware y carga/descarga de información de usuario y
Bloqueo de registros a través de una memoria USB.
6. Admite la vista fuera de línea de los registros de bloqueo.
7. Admite una visualización precisa de la hora y la fecha con una desviación anual inferior a dos
minutos.
8. Admite una conexión temporal con baterías de respaldo.
9. Puede configurar los bloqueos de huellas dactilares para que estén en el estado normalmente
abierto (NO) en
casos especiales.
10. Visualización de soporte del nivel de carga de la batería y generación de baja presión
alarmas

11. Cuenta con un diseño de mango de embrague eléctrico que ayuda a prevenir eficazmente el falla de bloqueo de huellas dactilares causada por daños a la estructura interna como resultado de la destrucción forzada del mango.

1.2 Lista de accesorios de instalación



Lista de accesorios de instalación

Nombre de número de serie	Cantidad	Unidad	Observaciones
01 Montaje del panel frontal	1	Establecer	
02 Cilindro de bloqueo	1	Establecer	
03 Eje cuadrado del mango 2		PC	
04 Cuerpo de la cerradura	1	Establecer	
05 Tapa de la batería	1	PC	
06 Baterías	4	PC	Cuatro piezas de AA alcalino baterías
07 Montaje del panel trasero	1	Establecer	
08 Tornillo	6	PC	Reserve dos tornillos y seleccione el tamaño de tornillo adecuado basado en el espesor de la puerta
09 Placa de sujeción trasera	1	PC	
10 Arandela impermeable	2	PC	Incluyendo el de la montaje del panel frontal
11 tornillos para vetas de madera	5	PC	
12 Tornillo para asegurar el cilindro	1	PC	
13 Placa de impacto	1	Establecer	
14 caja guardar	2	PC	
15 clave	2	PC	
16 Batería de respaldo		PC 9V	
17 Tarjeta de gestión	1	PCS Opcional	
18 Disco de instalación	1	PC	
Plantilla de perforación de 19 agujeros	1	PC	

1.3 Requisitos de instalación

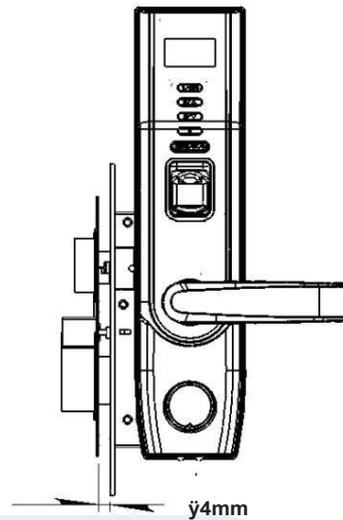
Precauciones:

1. La cerradura con huella dactilar es aplicable a puertas de 35 a 50 mm de grosor. Asegúrate de

Enumere sus requisitos especiales o comentarios para que se instalen bloqueos de huellas dactilares en puertas de más de 50 mm de espesor antes de realizar un pedido.

2. El espacio entre el cuerpo de la cerradura y la caja no puede exceder los 4 mm;

de lo contrario, debe adoptar una placa de revestimiento para asegurarse de que el espacio entre ellos no sea más de 4 mm, como se muestra en la siguiente figura:



3. Asegúrese de las direcciones de apertura de la puerta y el cuerpo de la cerradura. Suponga que usted es

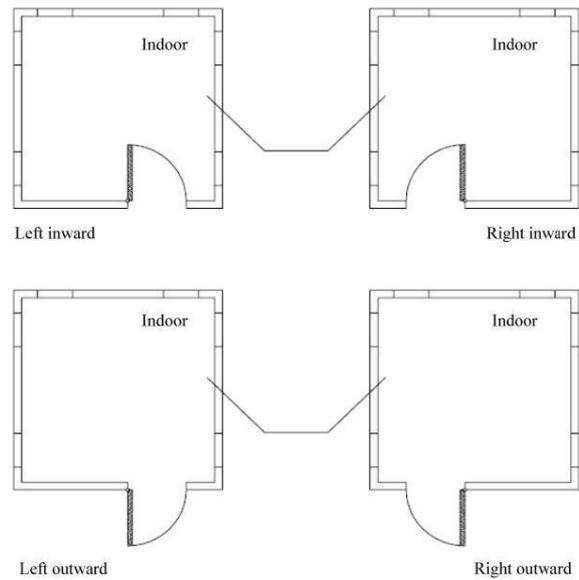
parado afuera y frente a una puerta y luego hay cuatro puertas que se abren

direcciones: izquierda hacia adentro, izquierda hacia afuera, derecha hacia adentro y derecha hacia afuera. Izquierda

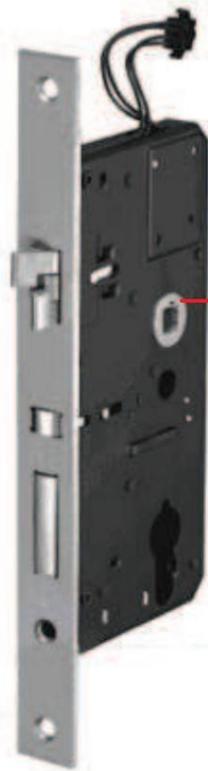
hacia adentro/hacia afuera significa que la puerta gira hacia adentro/hacia afuera con las bisagras a la izquierda;

derecha hacia adentro/hacia afuera significa que la puerta se abre hacia adentro/hacia afuera con las bisagras puestas

la derecha, como se muestra en la siguiente figura:



4. Asegúrese de que el punto central del mango esté aproximadamente a 1 m por encima del suelo.
5. Asegúrese de que el punto marcador del embrague esté justo encima del embrague.



El punto marcador está
justo encima del embrague.

6. Siga las instrucciones animadas para instalar bloqueos de huellas dactilares.

Herramientas recomendadas

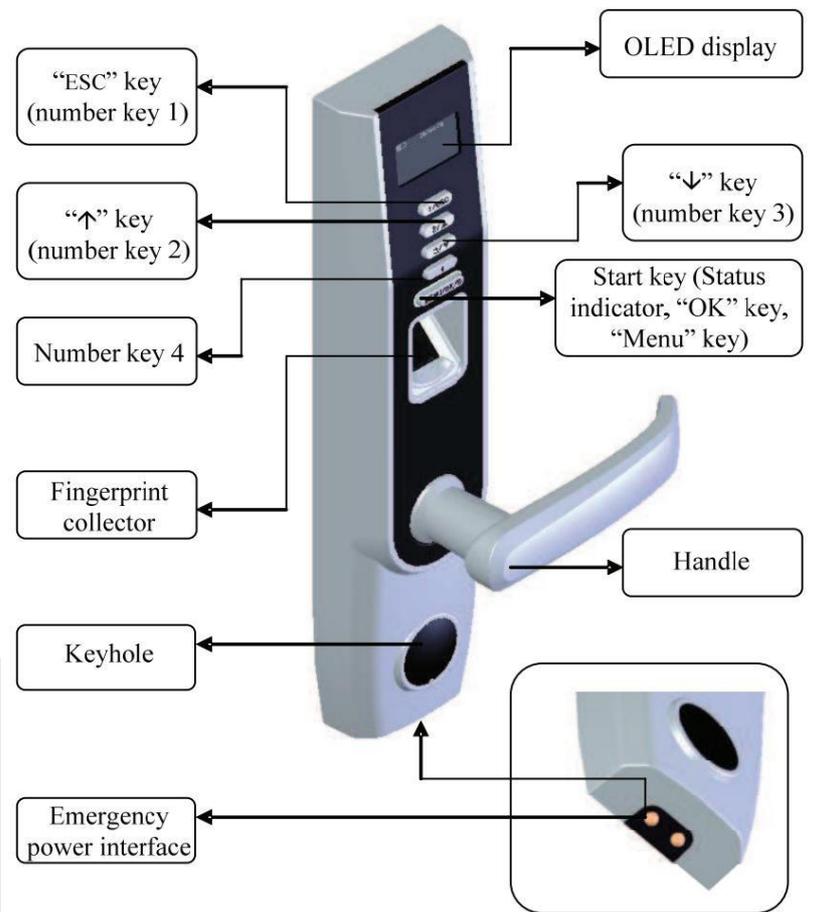
Es posible que necesite las siguientes herramientas mientras sigue las instrucciones para instalar

bloqueos de huellas dactilares:

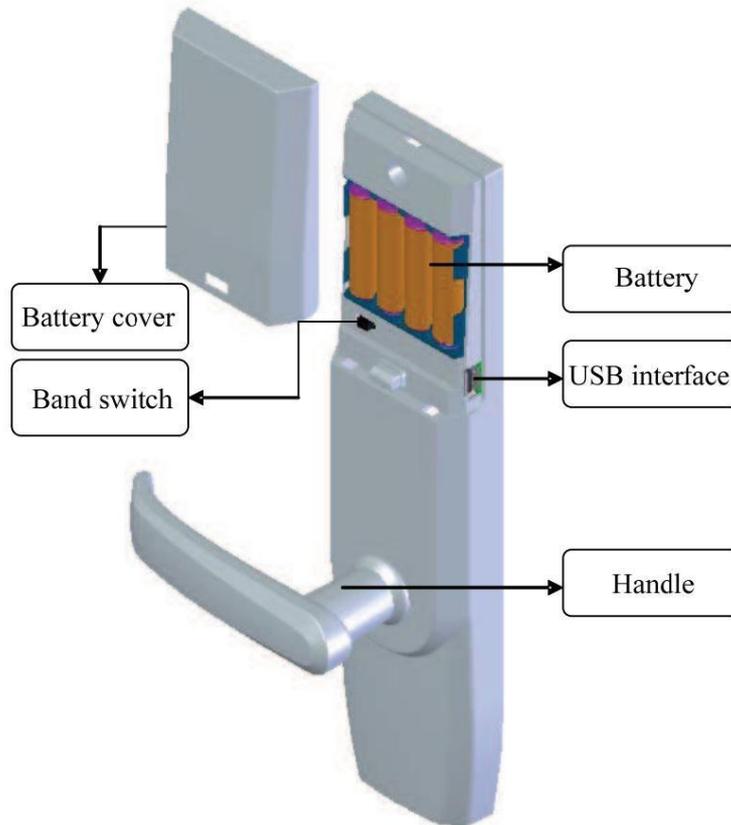
- z Una regla.
- z Un rotulador.
- z Una herramienta de perforación.
- z Un destornillador de estrella.

1.4 Vistas delantera y trasera

Vista frontal



Vista trasera



- Tecla ESC:** Presione esta tecla para salir de la operación actual y manténgala presionada. clave para apagar el bloqueo de huellas dactilares. La tecla ESC funciona como la tecla numérica "1".
- Tecla Ç:** Esta tecla se usa para aumentar manualmente (cuando se mantiene presionada, esta tecla aumentar rápidamente los valores de visualización) el valor de configuración o navegar entre las opciones del menú. La tecla Ç funciona como la tecla numérica "2".

tecla Ë:	Esta tecla se usa para disminuir manualmente (cuando se mantiene presionada, esta tecla disminuir rápidamente los valores de visualización) el valor de configuración o navegar entre las opciones del menú. La tecla Ë funciona como la tecla numérica "3".
Clave de inicio:	Esta tecla se puede utilizar para iniciar el bloqueo de huellas dactilares; presione y mantenga esta tecla durante tres segundos en la interfaz inicial para abrir el opciones de menú; esta tecla también funciona como confirmación (<OK>) llave.
Cambio de banda:	Si no puede acceder a las opciones del menú debido a la pérdida de administradores por alguna razón, proceda de la siguiente manera: Pulse y mantenga presionada la tecla Menú durante tres segundos para mostrar el administrador verificación, y luego gire el interruptor de banda en la parte posterior de la bloquear a la izquierda o a la derecha para abrir el menú como un súper administrador.
Indicador de estado:	puede despertar el bloqueo de huellas dactilares en estado inactivo presionando la tecla de inicio. El indicador LED verde parpadea cuando el el bloqueo de huellas dactilares funciona correctamente y el indicador LED rojo está encendido durante tres segundos si se produce un error. El indicador LED verde está encendido durante tres segundos cuando una operación tiene éxito.
Pantalla OLED:	la pantalla OLED en blanco y negro presenta gráficos en blanco o texto contra un fondo negro.
Sensor de huellas dactilares:	solo puede recopilar o unir huellas dactilares presionando su dedo(s) en el sensor de huellas dactilares cuando la luz en el la ventana del sensor de huellas dactilares se enciende; de lo contrario no pasa nada cuando presiona su(s) dedo(s) en el sensor de huellas dactilares.

#Nota: Cuando no puede apagar el bloqueo de huellas dactilares debido a la excepción de programa, mantenga presionada la tecla ESC para apagar y luego reinicie la huella digital cerrar. No se recomienda apagar el bloqueo de huellas dactilares presionando y manteniendo presionada la tecla ESC cuando el bloqueo de huella digital funciona normalmente.

Interfases de emergencia

Ojo de la cerradura: puede usar una llave mecánica para la apertura de puertas de emergencia.

Interfaz de alimentación externa temporal: puede adoptar una batería de respaldo externa para abrir la cerradura en caso de falla de desbloqueo debido a una fuente de alimentación insuficiente de el bloqueo de huellas dactilares.

interfaz USB

La interfaz USB se utiliza para la actualización del firmware y la carga/descarga del usuario. información y bloqueo de registros a través de un pen drive USB.

1.5 Precauciones

1. Le recomendamos encarecidamente que inscriba al menos un administrador después de instalar el bloqueo de huellas dactilares. Debe inscribir al menos a un administrador antes de inscribirse usuarios ordinarios.
2. No quite las baterías cuando haga coincidir, registre o elimine huellas dactilares porque el apagado repentino puede provocar la pérdida de datos de los bloqueos de huellas dactilares. Antes de quitar las baterías, asegúrese de que el bloqueo de huellas dactilares no esté funcionando. estado.
3. Se recomienda reemplazar las baterías de bloqueo de huellas dactilares al menos una vez cada seis meses para evitar dañar el circuito debido a la fuga de la batería. No utilice baterías de mala calidad.

4. Al instalar un bloqueo de huellas dactilares, conecte el enchufe al enchufe correctamente.

Una conexión incorrecta puede provocar una falla en el bloqueo de huellas dactilares.

1.6 Privilegios de usuario

Los privilegios de los usuarios se clasifican en tres tipos: superadministradores, administradores y usuarios comunes.

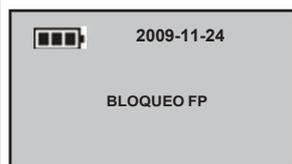
Súper administradores: se refieren a usuarios que tienen acceso a todas las funciones del sistema y modificar todos los ajustes del sistema.

Administradores: se refiere a los usuarios que tienen acceso a todas las operaciones excepto realizar configuración avanzada e inscripción de superadministradores.

Usuarios ordinarios: se refiere a todos los usuarios que no sean superadministradores y administradores. Los usuarios comunes solo tienen acceso a la coincidencia de huellas dactilares y funciones de desbloqueo.

1.7 Establecer hora

Debe establecer la fecha y la hora correctas en el primer uso de un bloqueo de huella digital en el siguientes pasos:

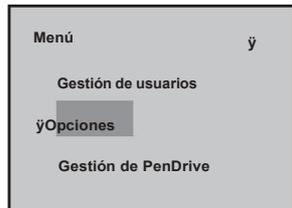


1) Encienda el bloqueo de huellas dactilares presionando el

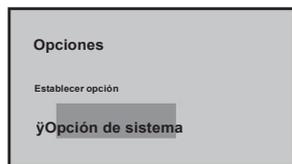
Tecla de inicio para abrir la interfaz inicial, como se muestra en la figura de la izquierda.

Nota la "  El icono " en la interfaz inicial es el icono de batería que indica cuánta carga queda.

En la esquina superior derecha de la interfaz inicial, el la pantalla alterna entre la fecha y la hora cada 5 segundos.

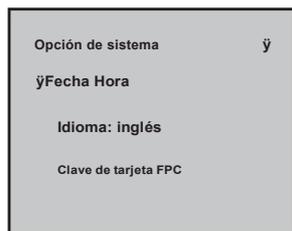


2) Mantenga presionada la tecla Menú durante tres segundos para acceder a la interfaz del menú. Pulse **↵** para seleccionar "Opciones" y presione OK para mostrar la configuración interfaz.

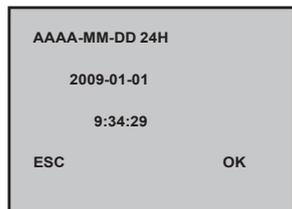


3) Presione **↵** para seleccionar "Sistema Opc." y luego presione

ESTA BIEN.



4) Presione OK para seleccionar "Fecha Hora".



5) Para modificar la fecha o la hora, presione **↵/↵** para mover el cursor a la opción deseada, y luego presione **↵/↵** nuevamente para ingresar la fecha u hora correcta. Pulse Aceptar para guardar tu configuración.

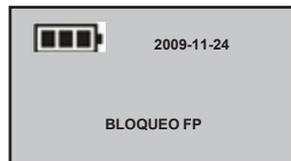
#Nota: Puede configurar la fecha entre el 1 de enero de 2003 y el 31 de diciembre de 2032.

Para programar la fecha fuera de este rango, es necesario consultar nuestro comercial representantes o ingenieros de soporte técnico de preventa.

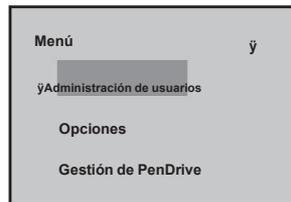
2. Inscripción y Verificación

2.1 Registrar un administrador

Si el bloqueo de huella no tiene administrador, al menos debe registrar uno administrador antes de inscribir a los usuarios normales. Para inscribir a un administrador, proceda como sigue:



1) Encienda el bloqueo de huellas dactilares presionando el Tecla de inicio para abrir la interfaz inicial. Presiona y mantenga presionada la tecla Menú para mostrar la interfaz del menú.



2) Pulse OK para mostrar la gestión de usuarios interfaz.



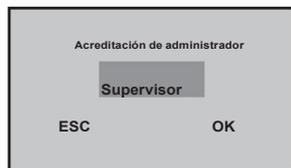
3) Presione \rightarrow para seleccionar "Admin Cnt" y luego presione ESTÁ BIEN.

Después de eso, el administrador inscrito puede realizar la huella digital, la contraseña y la tarjeta RF inscripción.

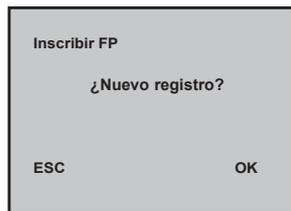
2.1.1 Registrar una huella digital



4) Presione y para seleccionar "Registrar FP" y luego presione OK.



5) Presione Y/y para seleccionar "Admin Accredit", y luego seleccione "Supervisor" (Superadministrador) o "Admin" (Administrador). Pulse Aceptar para confirmar tu seleccion.



6) Pulse Aceptar para continuar.



7) El sistema por defecto asigna ID de usuario no utilizados desde 00001 y también puede ingresar manualmente un ID de usuario no utilizado.

Este medidor se utiliza para indicar el éxito tiempos de inscripción de huellas dactilares. Una barra blanca se vuelve negra cada vez que registra una huella dactilar con éxito.



8) Presione el mismo dedo en el sensor de huellas dactilares tres veces consecutivas mediante la adopción de la adecuada modo de colocación de los dedos. El sistema le indicará para guardar la información de inscripción después de inscribirse la huella digital con éxito. Si la inscripción falla, el El sistema le pedirá que vuelva a registrar su huella digital.

El sistema regresa a la interfaz de "Nueva inscripción" después de una inscripción exitosa. Tú puede continuar o salir del registro de huellas dactilares.

#Nota: El último dígito en "00001-0" se refiere al conteo de huellas dactilares. "0" se refiere a la primera huella digital, "1" se refiere a la segunda huella digital y así sucesivamente.

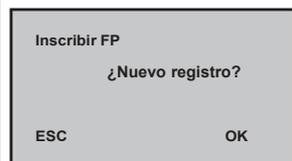
2.1.2 Registrar una contraseña



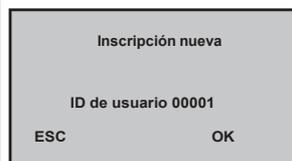
4) Presione **ÿ** para seleccionar "Enroll Pwd" y luego presione **ESTÁ BIEN**.



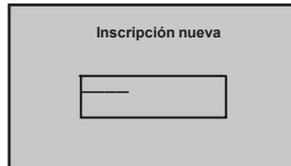
5) Presione **ÿ/ÿ** para seleccionar "Admin Accredit", y luego seleccione "Supervisor" (Superadministrador) o "Admin" (Administrador). Pulse Aceptar para confirmar tu seleccion.



6) Pulse Aceptar para continuar.



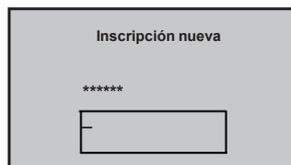
7) El sistema por defecto asigna ID de usuario no utilizados desde 00001 y también puede ingresar manualmente un ID de usuario no utilizado.



Inscripción nueva

[Numeric keypad input field]

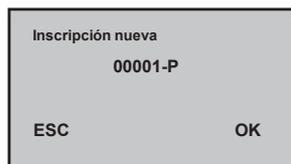
8) Ingrese una contraseña presionando las teclas numéricas y presione OK para confirmar su entrada.



Inscripción nueva

[Masked password input field]

9) Ingrese la contraseña nuevamente presionando el número y presione OK para confirmar su entrada. presiona OK después de la inscripción exitosa de la contraseña para volver a la Interfaz "Nueva Inscripción".



Inscripción nueva

00001-P

ESC OK

10) Pulse OK para guardar los datos registrados y salir de la registro de contraseña.

#Nota: Una contraseña consta de 6 a 10 dígitos. Puede inscribir solo una contraseña

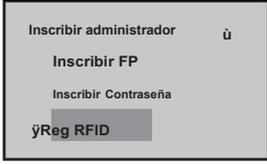
para cada ID de usuario y se permiten contraseñas repetidas; de lo contrario, el sistema mostrará el mensaje "Error de contraseña".

2.1.3 Registrar una tarjeta ID RF

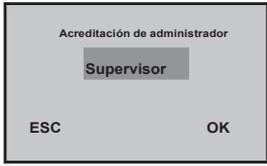
#Nota: esta función solo la proporcionan los bloqueos de huellas dactilares compatibles con RF

Función de tarjeta de identificación.

detalle



4) Seleccione "Registrar RFID" y presione OK.

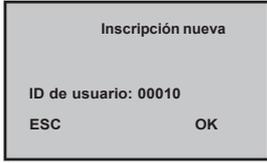


5) Presione Y/y para seleccionar "Admin Accredít", y luego seleccione "Supervisor" (Super administrador) o "Admin" (Administrador). Presione OK para confirmar su selección,

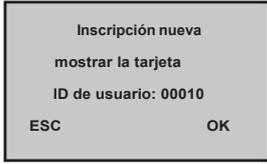
como se muestra en la figura de la izquierda.



6) Pulse Aceptar para continuar con el siguiente paso. La interfaz visualizado se muestra en la figura de la izquierda.



7) Ingrese el ID (entre 1 y 65534) a ser inscrito detrás de la opción "UserID", y presione OK, como se muestra en la figura de la izquierda:

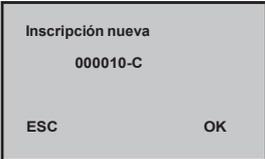


8) Muestre la tarjeta siguiendo las indicaciones, como se muestra en la figura de la izquierda:



Inscripción nueva
TARJETA: 16650449
ID de usuario: 00010
ESC OK

9) El número de tarjeta mostrado se muestra en la figura a la izquierda.



Inscripción nueva
00010-C
ESC OK

10) Pulse Aceptar para continuar con el siguiente paso. Los La interfaz mostrada se muestra en la figura de la izquierda.
Nota: La última letra "C" en "00010-C" se refiere a la ID tarjeta.

11) Presione OK para guardar los datos registrados y salir del registro de la tarjeta de ID.

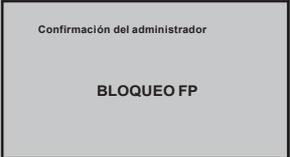
2.2 Registrar un Usuario Ordinario

Un administrador puede inscribir solo a usuarios comunes, con los siguientes pasos de operación:



2009-11-24
BLOQUEO FP

1) Encienda el bloqueo de huellas dactilares presionando el Tecla de inicio para abrir la interfaz inicial.



Confirmación del administrador
BLOQUEO FP

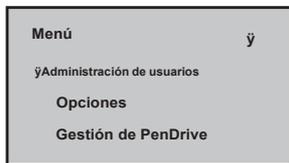
2) Mantenga presionada la tecla Menú para acceder al menú opciones A continuación, el sistema le pedirá que confirmación del administrador. Entra el administrador contraseña o haga coincidir su huella digital una vez. Pasemos a paso 4 si la verificación tiene éxito; de lo contrario, proceda a paso 3.



3) El sistema muestra el mensaje "Error Pwd". en la pantalla y volver a "Admin Affirm"

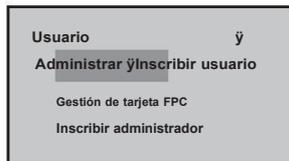
interfaz para la reverificación. El siguiente menú

la interfaz se muestra después de una verificación exitosa.



4) Pulse OK para mostrar la gestión de usuarios

interfaz.



5) Presione **↵** para seleccionar "Registrar usuario" y luego presione

ESTÁ BIEN.

Después de eso, el administrador inscrito puede realizar huellas dactilares, contraseñas y RFID.

inscripción de tarjetas. Los demás pasos de la operación son básicamente los mismos que los de

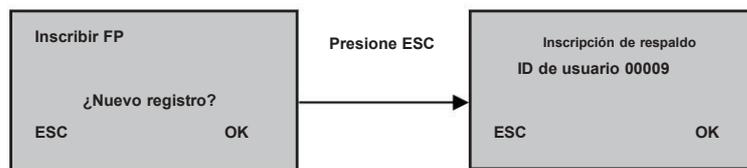
inscripción de administrador excepto que no tiene que seleccionar el administrador

privilegios Para obtener más información, consulte 2.1 Inscribir a un administrador.

2.3 Inscripción de respaldo

En el "¿Nuevo registro?" interfaz, si presiona ESC para cancelar la nueva inscripción, entonces la

Se mostrará la interfaz "Backup Enroll", como se muestra en la figura de la derecha.



Los pasos de inscripción de respaldo son básicamente consistentes con los nuevos pasos de inscripción excepto que "Inscripción de respaldo" en lugar de "Inscripción nueva" se muestra en la parte superior de la interfaz.

#Nota: 1. Es una sabia elección registrar las huellas dactilares de al menos dos

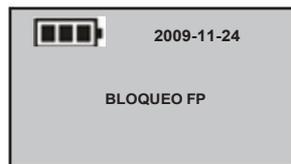
dedos para usuarios de larga data.

2. Si desea modificar la contraseña después de finalizar el registro de la contraseña, puede reemplazar la contraseña original con la contraseña ingresada en inscripción de respaldo.

3. Si realiza un registro de respaldo después de registrar la tarjeta RFID, el

El número de la tarjeta RFID original será reemplazado por el número de la tarjeta de identificación. ingresado en la inscripción de respaldo.

2.4 Establecer verificación de usuario y estado NO



- 1) Presione la tecla Inicio para mostrar la interfaz inicial.
El sensor de huellas dactilares está en estado activo.

- 2) Presiona tu dedo con la huella dactilar ya registrada o ingrese su contraseña (presione OK después de ingresar clave.)

Nota: Solo puede hacer coincidir las huellas dactilares cuando el bloqueo de huellas dactilares no está en estado NO.



- 3) Su número de identificación se mostrará en la pantalla después de la verificación exitosa y luego puede escuchar el sonido de desbloqueo. Gire el mango de la Bloqueo de huellas dactilares en 4 segundos para abrir la puerta.

Si la función NO está configurada en "SI" (Ver 3.1), el aparecerán indicaciones como se muestra en el paso 4 y el paso 5. se muestra después de una verificación exitosa; de lo contrario, no se mostrará ningún aviso.



- 4) Si presiona ESC cuando el sistema lo solicite si configurar la función NO, el bloqueo de huellas dactilares se bloqueará automáticamente. El icono de "Desbloqueo" en la pantalla cambiará al icono de "Bloqueo" y el sistema se apaga automáticamente.



5) Si presiona OK, la interfaz como se muestra en la aparecerá la figura de la izquierda, indicando ajuste NO exitoso. Mientras tanto, el timbre sonará tres veces consecutivas.

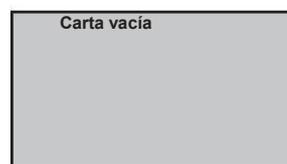
Si la verificación de huellas dactilares o contraseña no tiene éxito, el sistema mostrará un mensaje "Por favor, presione su dedo de nuevo" o "Error de contraseña". Los parámetros "Cantidad ilegal." y "Alarma ilegal" son configurados por el administrador. El sistema generar una alarma después de que las operaciones ilegales alcancen el valor especificado. Para detalles, ver 3.1.

#Nota: Si el valor del parámetro "Illegal Cnt." es mayor que 6, el sistema se apagará automáticamente si no verifica su huella digital o contraseña 6 veces consecutivas.

2.5 Gestión de tarjetas FP *

- #Nota:** 1) Esta función solo la proporcionan los bloqueos de huellas dactilares compatibles con Función de tarjeta Mifare.
- 2) Si no hay ningún administrador inscrito en el sistema, el sistema le pedirá que primero inscriba a un administrador.

Seleccione "FPCard Mng" en la interfaz "User Manage", como se muestra a continuación:



Crear PINCard: esta opción se utiliza para crear una tarjeta de identificación para un usuario que tiene ya ha sido inscrito en el bloqueo de huellas dactilares. puedes verificar su tarjeta de identificación en lugar de su huella digital (solo después de la el parámetro "Solo tarjeta" se establece en "Sí". Para más detalles, véase 3.1).

Registrar FPCard: esta opción se utiliza para almacenar una huella digital registrada directamente en la Tarjeta FP en lugar de en el bloqueo de huellas dactilares. Puede verificar el usuario identificar en forma de "Tarjeta FP + Huella digital", es decir, deslizar el Tarjeta FP antes de presionar el dedo.

Crear FPCard: esta opción se utiliza para duplicar las huellas dactilares registradas (almacenadas en el bloqueo de huellas dactilares) a la tarjeta FP. Puede verificar el usuario identidad ya sea a través de la "Huella digital" o en forma de "FP tarjeta + huella".

Carta vacía: Esta opción se utiliza para purgar todos los datos (huellas dactilares y números) almacenado en la tarjeta FP.

2.5.1 Crear una tarjeta PIN

1. Cree una tarjeta PIN

A cada usuario se le asignará un número de identificación, por ejemplo, 00001, después de que los usuarios sean inscrito en el bloqueo de huellas dactilares.



1) Seleccione "Administración de usuarios" Æ "Gestión de tarjetas PPC" Æ "Crear PINCard" en el menú principal. los

interfaz como se muestra en la figura de la izquierda esdesplegado:



2) Cuando se le solicite ingresar el número de ID de usuario, presione **Y/y** para seleccionar el ID de usuario deseado y presione **ESTÁ BIEN**. Luego, el sistema le solicita que "Mostrar el tarjeta" (Si el ID de usuario seleccionado no existe en el sistema, el sistema mostrará un mensaje "No Inscribirse"), como se muestra en la figura de la izquierda:



3) Pase su tarjeta FP por el lector de tarjetas.
z La interfaz, como se muestra en la figura de la izquierda:
Si el sistema muestra el mensaje "Escribir con éxito", su La tarjeta PIN se creó con éxito. Puedes reemplazar la verificación de la huella dactilar con la tarjeta PIN verificación.



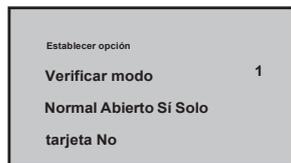
z Si la interfaz, como se muestra en la figura de la izquierda: su tarjeta PIN no está escrita en el sistema. "-7" significa error de escritura.

#Nota: Para crear una tarjeta PIN, debe asegurarse de que la ID de usuario ya exista en el sistema; de lo contrario, el sistema mostrará un mensaje "No inscribirse" y necesita repetir la operación. Una vez creada correctamente la tarjeta PIN, sólo el número de identificación se almacena en la tarjeta PIN.

2 Verifique la tarjeta PIN

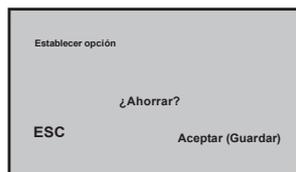
#Nota: Establezca el parámetro "Solo tarjeta" en "Si". Si configura el parámetro "Tarjeta

Solo" a "No", no puede verificar con la tarjeta PIN creada.



1) Seleccione "Establecer" /Æ "Establecer opción." desde el menú principal.

La interfaz como se muestra en la figura de la izquierda es desplegado:



2) Seleccione "Solo tarjeta" y presione OK. Luego presione Y/y para seleccionar "Si". Pulse Aceptar para guardar la configuración.

Luego, puede realizar la verificación de la tarjeta PIN.



3) Pase su tarjeta PIN por el lector de tarjetas

cuando el sistema vuelve a la interfaz inicial. Si

la interfaz como se muestra en la figura de la izquierda es

aparece, la tarjeta PIN se creó con éxito.

2.5.2 Registrar una tarjeta FP

1. Registrar una tarjeta FP



1) Seleccione "Administración de usuarios" /Æ "Gestión de tarjetas FPC" /Æ

"Registrar FPCard" en el menú principal para mostrar la

interfaz como se muestra en la figura de la izquierda:

<p>Registrar FPCard 00003-0 Coloque el dedo... ESC</p>	<p>2) Presione Y/y para seleccionar una ID y luego presione OK para confirme su selección y continúe con el siguiente paso. Coloque uno de sus dedos en el sensor de huellas dactilares.</p>
<p>Registrar FPCard 00003-0 Segunda pulsación ESC</p>	<p>3) Coloque el mismo dedo en el sensor de huellas dactilares otra vez.</p>
<p>Registrar FPCard 00003-0 Tercera Prensa ESC</p>	<p>4) Coloque el mismo dedo en el sensor de huellas dactilares por tercera vez.</p>
<p>Registrar FPCard 00003: 1 mostrar la tarjeta</p>	<p>La interfaz como se muestra en la figura de la izquierda es desplegado:</p>
<p>Registrar FPCard 00003: 1 Escribe éxito</p>	<p>5) Pase su tarjeta por el lector de tarjetas hasta que interfaz como se muestra en la figura de la izquierda es desplegado. Ahora la tarjeta FP está registrada con éxito.</p>

2. Verificar una tarjeta FP inscrita

Nota: configure la opción "Solo tarjeta" en No. Si la configura en Sí, la huella digital

lock solo verificará las tarjetas PIN de los usuarios.



1) En la interfaz inicial, deslice una tarjeta FP registrada a través del lector de tarjetas. Se muestra la interfaz como se muestra en la figura de la izquierda:



2) Coloca uno de tus dedos con huella dactilar inscrito en la ventana del sensor de huellas dactilares correctamente. Cuando la interfaz como se muestra en la figura de la izquierda se muestra, la tarjeta FP pasa la verificación exitosamente.

#Consejo: A través de las operaciones anteriores, solo almacena sus huellas dactilares en su tarjeta pero no en el bloqueo de huellas dactilares. Por lo tanto, debes mostrar tu tarjeta FP primero antes de la comparación de huellas dactilares. (Sus huellas dactilares solo se almacenan en su tarjeta FP.)

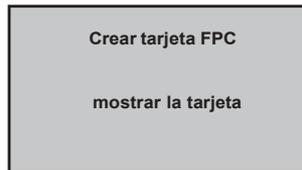
2.5.3 Crear una tarjeta FP

1. Crear una tarjeta FP

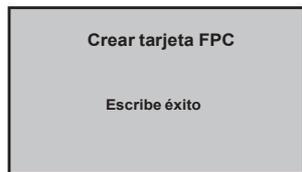
A cada usuario se le asigna una ID, por ejemplo, 00003, durante la inscripción de huella dactilar.



Seleccione "Administración de usuarios" / "Gestión de tarjetas FPC" / "Crear FPCard" desde el menú principal para mostrar la interfaz como se muestra en la figura de la izquierda:



2) Presione OK y la interfaz como se muestra en la se muestra la figura de la izquierda.



3) Pase su tarjeta por el lector de tarjetas hasta que la interfaz como se muestra en la figura de la izquierda es desplegado.
Ahora se crea correctamente una tarjeta FP.

2. Verificar una tarjeta FP creada

Nota: Configure la opción "Solo tarjeta" en No.

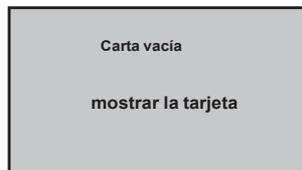
La operación de verificar una tarjeta FP creada es la misma que la de verificar una tarjeta FP inscrita.

#Consejo: A través de las operaciones anteriores, puede duplicar las huellas dactilares del

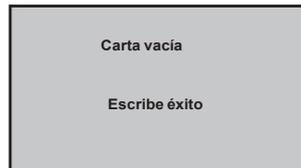
bloqueo de huella digital a una tarjeta FP. De esta manera, puede realizar la identificación ya sea mediante huella dactilar o "Tarjeta FP + huella dactilar". (Sus huellas dactilares se almacenan tanto en el bloqueo de huellas dactilares y su tarjeta FP).

2.5.4 Purgar una tarjeta FP

Para depurar toda la información en una tarjeta FP, proceda de la siguiente manera:



1) Seleccione "Administración de usuarios" /E "Gestión de tarjetas FPC" /E "Tarjeta vacía" en el menú principal para mostrar la interfaz como se muestra en la figura de la izquierda:



- 2) Pase su tarjeta por el lector de tarjetas hasta que la interfaz como se muestra en la figura de la izquierda es desplegado.
- Ahora la tarjeta FP se purga con éxito.

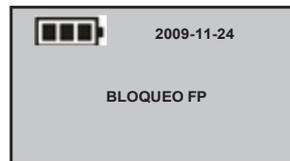
2.6 Eliminar datos de usuario



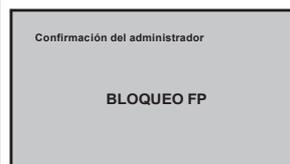
Advertencia:

Está prohibido apagar el bloqueo de huellas dactilares mientras se eliminan los datos del usuario para que para evitar que el programa borre accidentalmente otros datos.

Para eliminar los datos del usuario, proceda de la siguiente manera:



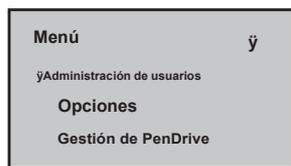
- 1) Presione la tecla de inicio para encender la huella digital bloquear y luego ingresar a la interfaz inicial.



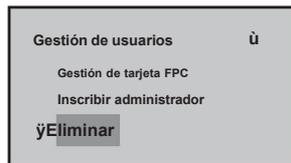
- 2) Ingrese la contraseña del administrador o la huella digital una vez. Si la verificación tiene éxito, vaya al Paso 4; de lo contrario, vaya al paso 3.



3) El sistema muestra el mensaje "Error Pwd". en la pantalla y vuelve a "Admin Affirm" interfaz para la reconfirmación. Si pasas el verificación, puede acceder a la interfaz "Menú".



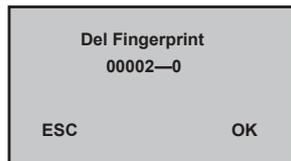
4) Presione OK para mostrar "Administrar usuarios" interfaz.



5) Presione ÿ para seleccionar "Borrar", y presione OK.

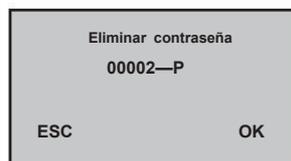


6) Pulse ÿ/ÿ para seleccionar el ID de usuario que desea eliminar y luego presione OK para confirmar su selección.



Si el usuario ha registrado sus huellas dactilares,

7) Pulse Aceptar para eliminar las huellas dactilares.



Si el usuario ha registrado una contraseña,

8) Presione OK para borrar la contraseña.



9) Confirmar la eliminación de este usuario. Pulse Aceptar para confirme la eliminación, o presione ESC para volver a la Interfaz de "Administración de usuarios".

10) Después de eliminar los datos del usuario, puede reiniciar el bloqueo de huellas dactilares y hacer coincidir el huellas dactilares eliminadas nuevamente para verificar si los datos del usuario se eliminaron con seguridad.

#Nota: Los administradores (incluidos los superadministradores) solo pueden eliminar usuarios ordinarios. Para eliminar una ID de administrador, debe seleccionar "Opciones" /E "Opciones de sistema". /E "Adv Option" /E "Clr Admin Pri", y luego seleccione "Administración de usuarios" /E "Eliminar" para eliminar la ID.

3. Información y configuración de la función de bloqueo

3.1 Ajustes de funcionamiento

Seleccione "Opciones" → "Establecer opción". del menú principal para mostrar lo siguiente información:

Establecer opción	Modo de verificación
Illega Alarma Si Illega	Normal Abierto Sí
Cnt. 10 Bloqueo	Solo Tarjeta No
5	1

Las opciones en "Establecer opción". incluyen: Illega Alarma, Illega Cnt., Bloquear, Verificar Modo, Normal Abierto y Solo Tarjeta.

Alarma ilegal (alarma ilegal): el bloqueo de huellas dactilares se apagará automáticamente

cuando el número de fallas de operación consecutivas excede el establecido valor. Después de reiniciar, su zumbador sonará de forma discontinua durante 30 segundos para generar una alarma de operación no válida y luego apagar automáticamente.

Illega Cnt. (Recuento de operaciones ilegales): este parámetro se utiliza para configurar el conteo de fallas de operaciones consecutivas. Una alarma de operación no válida se generará cuando el conteo de fallas consecutivas exceda el límite. Rango de valores: 3–99. Valor predeterminado: 10.

#El conteo de fallas se acumula cuando se inicia el bloqueo de huellas dactilares la próxima vez. Si

el número de fallas acumuladas excede el umbral, el bloqueo de huellas dactilares generará una alarma de operación no válida; de lo contrario, el conteo de fallas no ya no se acumulará después de un desbloqueo exitoso.

Cerrar: Este parámetro se utiliza para establecer la duración de la coincidencia exitosa para desbloquear Seleccione Bloquear y presione OK para mostrar el Bloqueo interfaz. Pulse Y/y para seleccionar un valor. Presione ESC para salir actual interfaz y guarde su configuración. Para este parámetro, su unidad de la cantidad es 1 segundo y el rango de valores es 3–15, es decir, 3–15 segundos.

#Nota: La unidad de cantidad y el valor máximo de este parámetro aquí son configuraciones estándar. Si necesita valores de parámetros más grandes, consulte nuestros representantes comerciales o ingenieros de soporte técnico de preventa.

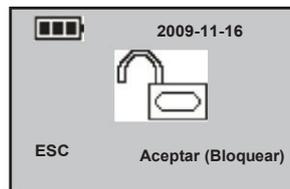
Modo Verificar: Presione OK para mostrar la interfaz del Modo Verificar, y presione Y/y para seleccione un valor. Hay tres valores opcionales 0, 1 y 2 que representan diferentes modos de coincidencia respectivamente, y el valor predeterminado el valor es 1

Modo de verificación 0: solo el administrador puede abrir la cerradura, mientras que el desbloqueo La función está deshabilitada para los usuarios normales.

Modo de verificación 1: este es un modo de coincidencia predeterminado. Los usuarios pueden abrir la cerradura haciendo coincidir con éxito sus huellas dactilares solo una vez.

Modo de verificación 2: Este es un modo de verificación dual. El administrador puede abrir el bloqueo al hacer coincidir con éxito su huella dactilar solo una vez, pero un el usuario normal tiene que pasar la verificación en dos coincidencias cualesquiera modos utilizando el mismo ID.

Abierto normal: Presione OK para mostrar la interfaz de Abierto normal y presione Y/y para seleccione Sí o No. Si selecciona Sí, se mostrará un mensaje después de desbloqueo, preguntándole si desea seleccionar Normal Open. Si presiona OK, el sistema le indicará que la función NO está habilitado y luego se apaga automáticamente e inmediatamente. los La interfaz abierta normal se muestra de la siguiente manera:

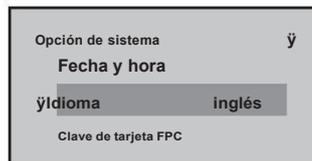


Para deshabilitar la función NO, encienda el sistema y presione OK en la interfaz abierta normal. Entonces el sistema cierra la cerradura y se apaga automáticamente.

Solo tarjeta: Pulse OK para mostrar la interfaz Sólo tarjeta y pulse Y/y para seleccione Sí o No. Si selecciona Sí, solo necesita verificar su ID tarjeta. +Si selecciona No, debe verificar tanto su tarjeta de identificación como huella dactilar.

3.2 Configuración de idioma

Seleccione "Opciones" → "Opciones de sistema". Æ "Idioma" en el menú principal para mostrar la siguiente información:



Presione OK para mostrar la interfaz de idioma y presione Y/y para seleccionar el idioma deseado. idioma. Presione OK para confirmar su configuración y luego presione ESC para salir de System Opt. Cuando el sistema le pregunte si desea guardar su configuración, presione OK y su configuración surtirá efecto después de reiniciar el sistema.

#Nota: La selección de idioma es una función no estándar. Si necesita esta función,
por favor consulte a nuestros representantes comerciales o soporte técnico de preventa
ingenieros

3.3 Contraseña de la tarjeta FP

Después de configurar una contraseña para su tarjeta FP, el bloqueo de huella digital escribirá esto
contraseña en una tarjeta Mifare durante la inscripción o creación de su tarjeta FP.

Seleccione "Opciones" → "Opciones de sistema". → "Clave de tarjeta FPC" en el menú principal para mostrar
la siguiente información:

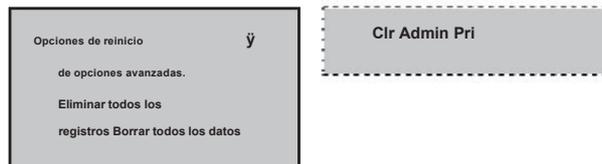


La contraseña de la tarjeta FP consta de 6 dígitos. Para ingresar una contraseña, primero seleccione
un dígito del 0 al 9 presionando Ç o È (puede mantener presionada Ç o È para desplazarse rápidamente
a través de los 10 dígitos) y presione OK para confirmarlo. Luego ingrese el siguiente dígito en el
de la misma manera hasta el último. Finalmente, presione OK para confirmar la contraseña y regresar a
el Sistema Opt. menú.

3.4 Configuración avanzada

#Nota: Solo el superadministrador tiene derecho a realizar configuraciones avanzadas.

Seleccione "Opciones" → "Opciones de sistema". → "Opción avanzada" en el menú principal para mostrar
la siguiente información:



Las opciones en "Opción avanzada" incluyen: Restablecer opciones, Borrar todos los registros, Borrar todo Datos y Cnr Admin Pri. Seleccione cualquiera de estas opciones y presione OK para mostrar la interfaz de configuración relacionada. Presione OK de acuerdo con el aviso para confirmar su configuración y volver a la interfaz de opciones avanzadas, o presione ESC para salir de la interfaz actual sin realizar ninguna operación.

Restablecer opciones: Este parámetro se utiliza para restaurar el bloqueo de huellas dactilares a la fábrica valores predeterminados

Del All Logs: este parámetro se utiliza para eliminar todos los registros de verificación de un chip de memoria.

Borrar todos los datos: este parámetro se utiliza para eliminar todas las imágenes de huellas dactilares registradas, contraseñas y registros.

Cnr Admin Pri: este parámetro se utiliza para cambiar un administrador a un ordinario usuario. Esta función debe utilizarse con precaución. Es recomendado para registrar al menos un nuevo administrador a tiempo después de borrar el prioridad de un administrador.

3.5 Explorar información del sistema

Los usuarios pueden navegar por toda la información del sistema, incluida la huella digital registrada conteos, usuarios inscritos e información del dispositivo. Seleccione "Información del sistema" en el menú principal, y presione OK para continuar con el siguiente paso y mostrar la siguiente información:

Información del sistema	ÿ
Examinar registros	
Registrar usuario	5
Inscribir FP	1

Tronco	85
Centro de administración	2
Contraseña Usr	3
Registro RFID	12
Información de espacio libre	
Información del desarrollador	

Presione ÿ/ÿ para seleccionar Free Space Info y luego presione OK para navegar por los siguientes información:

Información de espacio libre	
Cnt FP	499
Tronco	29915
Registro RFID	488

#Nota: Solo los bloqueos de huellas dactilares compatibles con tarjetas de identificación están configurados con el Opciones "Registrar FPID" e "Información de espacio libre".

Presione ÿ/ÿ para seleccionar Dev Info y luego presione OK para explorar los siguientes información:

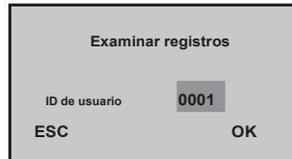
Información del desarrollador	ÿ
FPCnt(100)	5
Registro (10k)	3
hora manu	

Número de serie
Vendedor
Nombre del dispositivo
Versión de algoritmo
Versión de firmware

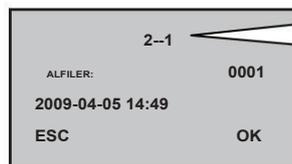
3.6 Examinar registros

Los bloqueos de huellas dactilares admiten la navegación fuera de línea de los registros de desbloqueo, que facilita a los usuarios verificar si hay algún desbloqueo excepcional a tiempo.

Seleccione "Examinar registros" en el menú principal para mostrar la siguiente información:

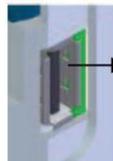


Presione Y/y para seleccionar un número registrado que desea buscar en los registros y luego presione OK para confirmar la fecha y hora del registro:



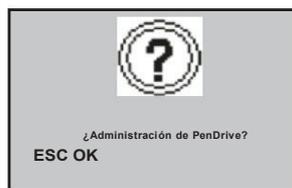
El primer dígito denota el número total de registros y el último denota el registro actual.

3.7 Gestión de memorias USB

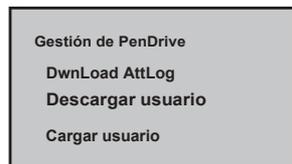


interfaz USB

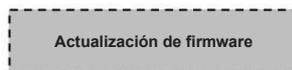
1) Inserte una memoria USB en la interfaz USB.



2) Seleccione "PenDrive Mng" en el menú principal y presiona OK. Se muestra un mensaje como el que se muestra a continuación.



3) Pulse Aceptar en el cuadro de diálogo de solicitud para mostrar el siguiente interfaz:



1. Descargar registros de asistencia



1) Presione **Y/y** para seleccionar "Dwn AttLog" y luego presione **ESTÁ BIEN**. Cuando finalice la descarga, aparecerá lo siguiente se muestra la interfaz:

2) Presione **ESC** para volver a la interfaz inicial y luego retire la memoria **USB**.

Ahora la memoria **USB** almacena dos archivos: **X_attlog.dat** (registros de asistencia) y **X_user** (donde "X" indica que el número de dispositivo es X).

#Consejo: si la descarga se realiza correctamente, aparecerá el mensaje "Copiar datos Suc". Si el

el sistema muestra el mensaje "¿Conectar Pen Drive?", Verifique si el **USB pen drive** está enchufado correctamente.

2. Descargar datos de usuario

La descarga de datos de usuario es similar a la descarga de registros de asistencia. Pulse **Y/y** para seleccionar "DwnLoad User" en el menú "PenDrive Mng". Los archivos **user.dat** (usuario información) y **template.dat** (plantilla de huellas dactilares) serán simultáneamente descargado en la memoria **USB**.

3. Cargar datos de usuario

Presione **Y/y** para seleccionar "Cargar usuario" en el menú "PenDrive Mng" y luego presione **ESTÁ BIEN**. Los archivos **user.dat** (información del usuario) y **template.dat** (plantilla de huellas dactilares) almacenados en la memoria **USB** se cargarán simultáneamente en el bloqueo de huellas dactilares.

#Consejo: si un usuario sale con la misma ID en el bloqueo de huellas dactilares, la nueva carga sobrescribirá los datos de usuario existentes; de lo contrario, los datos del nuevo usuario serán añadido directamente.

4. Actualización de firmware

Puede seleccionar "Actualizar firmware" para actualizar el firmware de un bloqueo de huellas dactilares a través de los archivos de actualización en la memoria USB.

#Nota: si necesita archivos de actualización de firmware, comuníquese con nuestro soporte técnico ingenieros Por lo general, no se recomienda actualizar el firmware.

Sugerencia: no realice operaciones no válidas (por ejemplo, inserte o extraiga la memoria USB con frecuencia o durante la carga/descarga) en la memoria USB, ya que puede provocar inestabilidad en el sistema. Se recomienda mantener la puerta abierta durante el uso de la memoria USB.

4. Convenciones sobre otras funciones

4.1 Indicaciones de funcionamiento de rutina

Indicación de éxito de la operación del usuario: el zumbador suena una vez y el LED verde el indicador permanece fijo durante 3 segundos.

Indicación de falla de operación del usuario: El zumbador suena un tono corto dos veces y el rojo El indicador LED permanece encendido durante 3 segundos.

Indicación de advertencia: El zumbador suena un tono corto cinco veces de forma intermitente.

4.2 Prevención de pérdidas del administrador

Para evitar fallas en la operación del menú como resultado de la pérdida del administrador, puede tomar las siguientes medidas: Mantenga presionada la tecla Menú durante 3 segundos para mostrar la interfaz de verificación del administrador. Luego mueva el interruptor de banda en la parte trasera del Bloqueo de huellas dactilares a la izquierda o a la derecha. Ahora puedes acceder a los menús como super administrador para la gestión y operación.

4.3 Protección de bajo voltaje de la batería

Protección de bajo voltaje: cuando el medidor de la batería permanece en una barra, el sistema le indica que reemplace la batería y el icono de la batería comienza a parpadear. si presionas y mantenga presionada la tecla Menú, el sistema le indicará que no puede acceder a los menús. En

Además, los menús también son inaccesibles durante el uso de energía externa para evitar la pérdida de datos causada por la inestabilidad de energía. Cuando el medidor de la batería permanece por debajo de una barra, la batería se apaga automáticamente.

4.4 Salida automática del programa y apagado del sistema

El bloqueo de huellas dactilares se apaga automáticamente al coincidir con éxito y desbloqueo

El bloqueo de huellas dactilares se apaga automáticamente cuando establece Sí para el Opción "Normalmente abierto" al desbloquear.

El bloqueo de huellas dactilares se apaga automáticamente cuando el número de inválidos operaciones supera el umbral. El bloqueo de huellas dactilares se apaga automáticamente cuando se genera una alarma durante 30 segundos al reiniciar.

El bloqueo de huellas dactilares se apaga automáticamente cuando el voltaje de suministro es menor que el voltaje de detección de nivel 3.

El bloqueo de huellas dactilares se apaga automáticamente si no se pulsa ninguna tecla dentro 10 segundos en la interfaz inicial.

4.5 Descripción del uso de energía externa

El bloqueo de huellas dactilares admite el uso temporal de alimentación de CC externa para huellas dactilares o coincidencia de contraseña y desbloqueo, pero cuando se conecta con una batería externa, el

El bloqueo de huellas dactilares no puede proporcionar funciones especiales como inscripción, eliminación y configuración, a fin de evitar la pérdida de datos como resultado de la inestabilidad de energía.

Como se muestra en la figura a continuación, conecte una batería de 9 V a los dos puntos de acceso en el parte inferior de una cerradura de huella digital, independientemente de la polaridad.

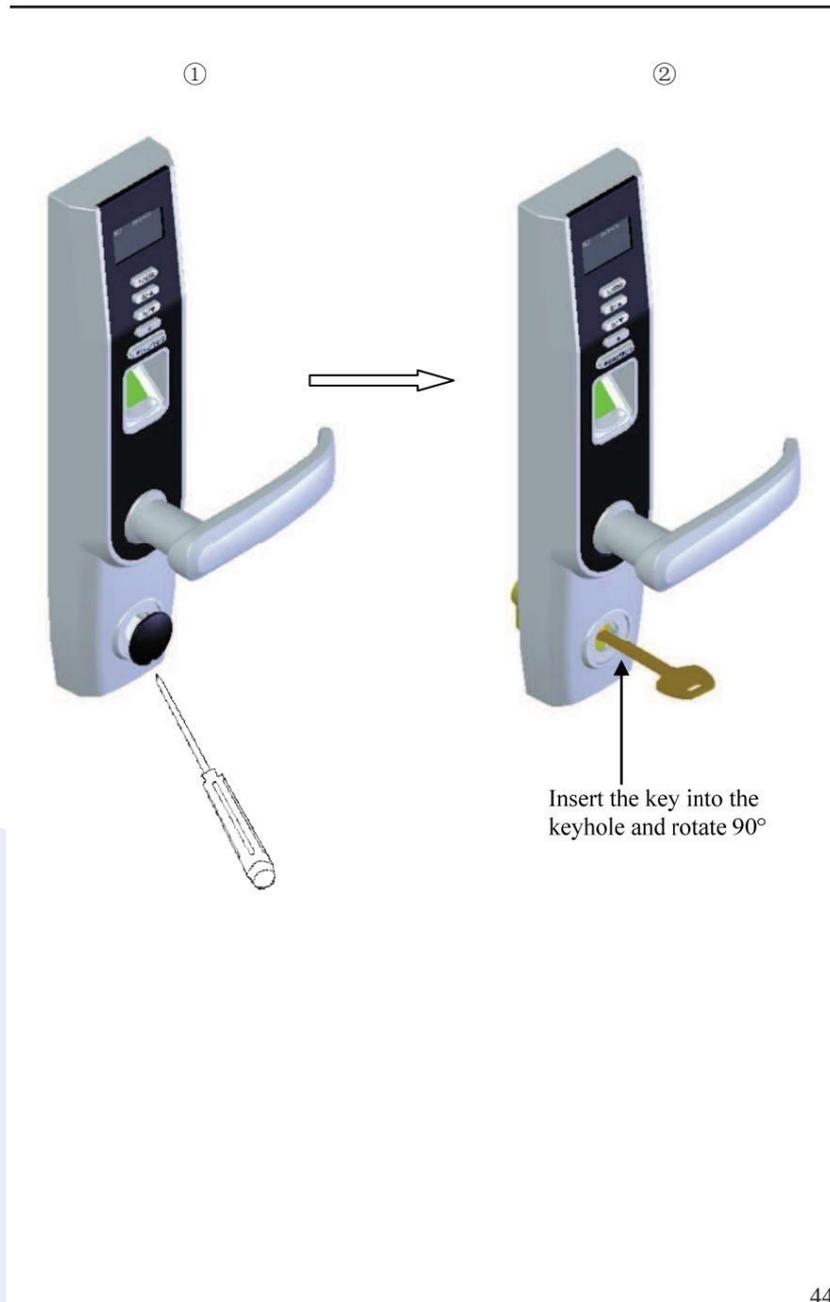


Si apaga un bloqueo de huellas dactilares sin cerrar el bloqueo durante el uso de alimentación externa, el cilindro de la cerradura no volverá automáticamente a su posición original. Es decir, el bloqueo de huellas dactilares permanece en estado NO. Para resolver este problema, puede reemplazar la batería y luego abra la cerradura una vez para tener el cilindro de la cerradura en su lugar.

4.6 Desbloqueo con llave mecánica de emergencia

Puede abrir la puerta con una llave mecánica de emergencia en caso de que la electrónica componente no funciona.

- (1) Haga palanca para abrir la tapa del ojo de la cerradura insertando el extremo afilado de un bolígrafo o destornillador con un diámetro de menos de 3 mm. Retire la cubierta.
- (2) Inserte la llave de emergencia en el ojo de la cerradura y gírela 90° para desbloquear.



Apéndice

Especificaciones técnicas

Sensor ¼: Sensor óptico sin recubrimiento

¼ Capacidad: 500 imágenes de huellas dactilares; 100 contraseñas; 500 usuarios.

¼ Modo de coincidencia: coincidencia de huellas dactilares, coincidencia de contraseña, tarjeta MF e ID
emparejamiento de cartas.

¼ Capacidad de registro: 30000

¼ Resolución: 500 DPI

¼ Velocidad de identificación: 2 segundos

¼ Tasa de falsa aceptación: 0.0001% ¼ Tasa

de falso rechazo: 1%

¼ Potencia: cuatro pilas AA; voltaje de trabajo: 4.2V-6V. ¼ Recuento de bloqueo: 4000 (cuatro pilas alcalinas NANFU)

¼ Temperatura: 0-45°C

¼ Humedad: 10%-80%



Dirección: Blvd Antonio L. Rodriguez n°3000, Piso 11-Of.1101-
Torre Albia, Col.Santa Maria, Mty -N.L. C.P. 64650, Mexico
/Email: ventas@bluemetric.mx/ (81)8315 5764