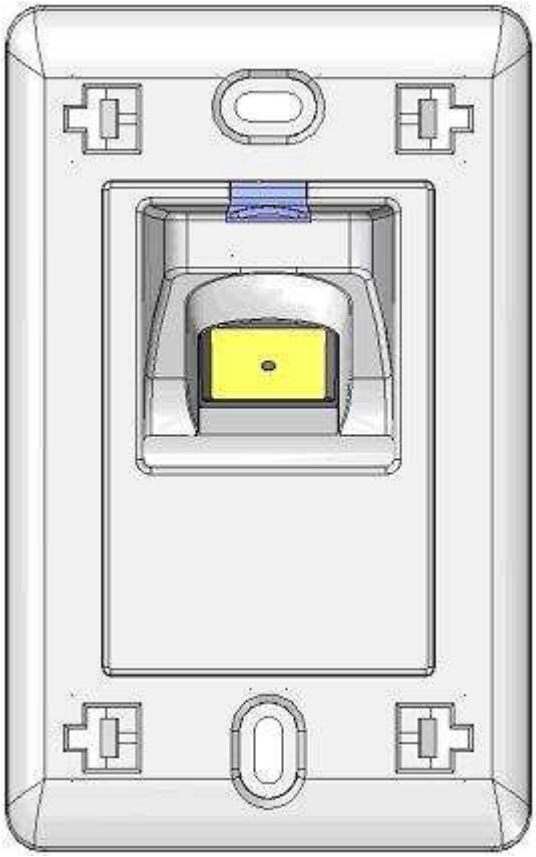
BioB Guía de usuario

Versión -1.00



UNION COMMUNITY

<Revisiones>

Versión	Fecha	Descripción	Versión firmware
1.00	2014-08-06	Versión inicial	10.61.00-000.16
1.01	2014-08-07	Valores por defecto modificados	
1.04			

< Glosario >

- Admin, Administrador
  - Usuario que puede acceder al menú del terminal y puede añadir/modificar/borrar usuarios de terminal y cambiar el funcionamiento cambiando la configuración.
  - Si no hay administrador de terminal, cualquiera puede cambiar la configuración, así que es recomendable registrar al menos un administrador.
  - Debe tener cuidado con el registro y operativa porque un administrador tiene el privilegio de cambiar parámetros críticos de funcionamiento en la unidad de reconocimiento dactilar.

- Método autentificación
  - Diferentes modos de autentificación incluyendo FP (huella dactilar), RF (tarjeta) o una combinación de ambos métodos.
  - Card or FP: se puede utilizar la tarjeta o la huella para identificarse.
  - Card & FP: debe utilizar la tarjeta y la huella para identificarse.

- Botón timbre
  - Utilizado para activar una campana, dispositivo o telefonillo que se conecta externamente al dispositivo.

Índice

1. Lectura previa al primer uso

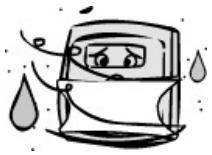
1.1. Precauciones de seguridad

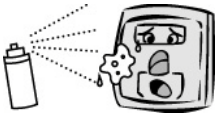
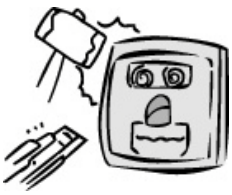
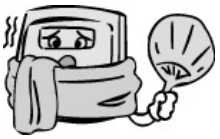
- Aviso

No manipule la unidad con las manos húmedas y no permita que se vierta algún líquido dentro. Puede provocar un cortocircuito o daño.		No sitúe una fuente de fuego cerca de la unidad. -> Puede causar un incendio.	
No desmonte, repare o modifique la unidad. Puede causar un cortocircuito, fuego o daño.		No permita que los niños se acerquen. Puede causar un accidente o daño.	

- Si las instrucciones mostradas no son seguidas, puede causar la muerte o serios daños al usuario.

- Precaución

Aleje el terminal de una fuente directa de sol. Puede causar mal funcionamiento, deformación o cambio de color de la unidad.		Evite la humedad alta y el polvo. Puede provocar un mal funcionamiento de la unidad.	
Evite utilizar agua, benceno, disolvente o alcohol para limpiar la unidad. Puede provocar un cortocircuito o fuego.		No acerque un imán a la unidad. Puede dañarla o provocar un mal funcionamiento.	

Evite tener el área de captura de huella sucia. Puede provocar una autentificación incorrecta de las huellas dactilares 	Evite utilizar insecticidas o espráis inflamables cerca de la unidad. Se puede deformar o cambiar el color de ésta. 
Evite los golpes y el uso de objetos cortantes en la unidad. Esta puede dañarse o romperse. 	No situé la unidad en lugar con cambios bruscos de temperatura. Puede provocar malfuncionamiento de ésta. 

- Si ignora las precauciones arriba referenciadas, puede producirse un daño o accidente humano.

※ Bajo ninguna circunstancia Union Community (Sticard) será responsable de los accidentes o daños provocados por un uso inapropiado del producto. Debe seguir las indicaciones establecidas en esta guía de usuario.

1.2. Especificaciones

Elemento	Especificación	Observaciones
CPU	32Bit RISC CPU(400MHz)	
RTC	CPU RTC / Batería litio	Fecha/Hora para logs
Tecla timbre	Sensor táctil capacitativo	Activar salida timbre
LED	3 Colores (rojo, verde, azul)	
Buzzer	Audible feedback buzzer	
Memoria	64M SDRAM	
	4M NOR Flash	1,000 usuarios (1,000 huellas)
Sensor huella	Optical	
Velocidad autentificación	<1 sec.	
Área escaneo / Resolución	13.2 * 15.2 mm / 500 DPI 260*300	
FRR / FAR	0.1% / 0.001%	
Temperatura / Humidad		
Amperaje	Standby: 80mA Máxima: 250mA	
Transformador AC / DC	ENTRADA : Universal AC 100 ~ 250V	
	SALIDA: DC 12V	
	Aprobada UL, CSA, CE	
Puerto comunicación	Bluetooth: Bluetooth v2.1 + EDR Alimentación salida Class 2	Aplicación smartphone B-UNIS
	RS-485	BLC015/LC010
	Salida Wiegand	26/34 bit Wiegand
Cerradura	Cerradura normalmente cerrada / abierta	Cerradura puerta
Monitorización	Entradas M0, M1	Control puerta
Inside Open	IO	Entrada botón salida
Salida timbre	Bell A/B Amperaje Máximo = 60mA	Salida telefonillo / timbre
Lector tarjeta	125KHz RF (opcional) 13.56MHz SC	
Tamaño	72mm * 111mm * 41.4mm	

1.3. Descripción del equipo

1.4. Funcionamiento LED

●	Error	Azul	Luz apagada : Normal Luz encendida : Fallo en autenticación
●	Correcto	Verde	Luz encendida: Tarjeta o autenticación correcta de la huella dactilar. Se encenderá durante el periodo de apertura de la puerta.
●	Stand by	Azul	Parpadeo : conectado al smartphone por bluetooth Luz encendida: Cuando el LED esté encendido, se establece en la configuración del terminal.

1.5. Funcionamiento del timbre

Normal	Cuando se presiona emite pitido y la salida de timbre se activará (Funcionamiento de timbre)
Parametros iniciales	1) Dar corriente 2) Mantenga pulsada la tecla de campana durante 2 segundos para que suene.

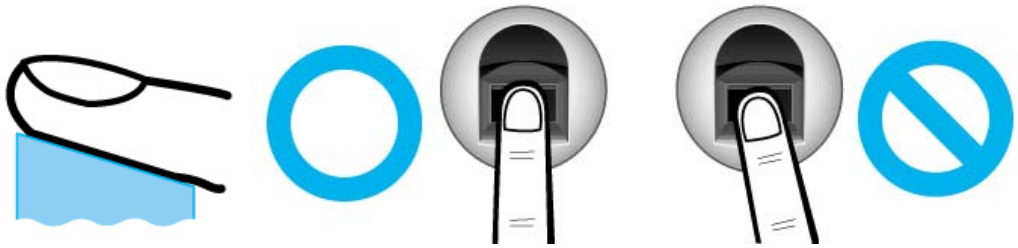
1.6. Sonido-zumbador durante el funcionamiento

“beep”	Al presionar el botón de la campana o pasando tarjeta	Cuando se pulsa un botón o una tarjeta se está leyendo Cuando se termina la entrada de huellas dactilares , lo que permite al usuario retirar su huella dactilar
“beep beep”	Fallo	Fallo de autenticación o mal uso
“beep,beep beep”	Correcto	Autenticación correcta o configuración completa para el usuario actual

1.7. Métodos de registro de huellas dactilares y de entrada correcta

- Método correcto de registro de huellas

Coloque el dedo índice en el sensor tal y como se muestra en la imagen siguiente.
Tocar sólo con la punta del dedo no es método de registro apropiado.
Asegúrese de que el centro de su dedo toque el sensor.



- Use su dedo índice.

  El dedo índice garantiza una entrada precisa y estable de la huella dactilar.

* Compruebe que su huella es clara y no está dañada.

Es difícil reconocer huellas en los dedos secos, húmedos, poco claros o dañados (corte, ezcema, quemadura…)

Use otro dedo en dichos casos.

- Precauciones acerca de las condiciones en las huellas dactilares

  Dependiendo del estado de la huella dactilar del usuario, éstas pueden no ser útiles o causar problemas.

  - Si la huella es poco clara o está dañada, no puede ser reconocida.
    En ese caso, utilice otro dedo o una tarjeta.

  - Cuando el dedo está seco, sobre sobre el dedo para un mejor funcionamiento.

  - Para los niños, puede ser muy difícil o imposible el uso del lector, ya que las huellas son demasiado pequeñas o claras. Es recomendable registrar sus huellas cada seis meses.

  - Para las personas mayores puede que no sea posible registrar sus huellas, si hay demasiadas líneas finas (arrugas) en ellas.

  - Se recomienda registrar más de dos huellas por persona.

2. Introducción

2.1. Descripción

BioB es un dispositivo de control de acceso de montaje empotrado . Puede ser utilizado en aplicaciones de pequeña / mediana empresa o control de acceso residencial. Proporcionará acceso a un área segura utilizando una huella dactilar registrada o tarjeta.

BioB comunica mediante la tecnología Bluetooth con la aplicación B- UNIS para el usuario y la gestión de registros

2.2. Características

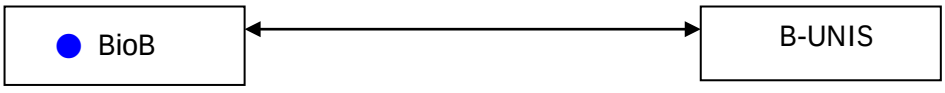
- **Comunicación Bluetooth v2.0**
  - Instalación sencilla utilizando la aplicación de smartphone B-Unis
    - Gestión.
    - Actualización del Firmware.
    - Gestión de usuarios.

- **Sensor Optico de huellas dactilares**
  Detección automática – Proceso simple de autenticación sin clave.
  Detección de dedo vivo(LFD) – Nivel LFD programable para detectar huellas dactilares reales / falsas.

- **Lector de tarjetas**
  Lector de tarjeta inteligente 13,56 MHz o lector de 125KHZ RF opcional.
- **Timbre**
  - Tecla táctil capacitiva para activar un telefonillo de puerta / timbre conectado externamente para los visitantes.

2.3. Configuración

2.3.1. Configuración independiente



Por favor, consulte la Guía del usuario B- UNIS SmartApp para obtener información de configuración y conexión.

Establecer conexión Bluetooth para teléfono inteligente aplicación B- UNIS.

- Nombre del dispositivo: FMD10_99999999

- B-UNIS Contraseña: 9999

- Contraseña emparejamiento: 0000 (Primera conexión)

- Configuración básica cuando se libera de fábrica.

NOTA : Si la contraseña de B- UNIS se pierde y no se puede conectar al BioB debe inicializarse a los valores de fábrica.

3. Configuración del entorno

3.1. Parámetros

Los parámetros de configuración se establecen a partir de la aplicación B- UNIS Smartphone:

Terminal/Nombre del dispositivo: 1-30 caracteres
El nombre del BioB para identificar el dispositivo por Bluetooth.
Por defecto: FMD10_99999999

Timbre : ON/OFF
Esto es para controlar la salida de zumbador.
Por defecto: ON

Estado del LED Bluetooth: Habilitar/Deshabilitar
Si se activa el LED azul parpadeará cuando esté conectado correctamente a la aplicación B-UNIS.
Por Defecto: ON

LED Azul: Habilitar/Deshabilitar
Si habilita el LED azul siempre estará encendido y si está conectado a la aplicación B- UNIS el LED azul se apagará. Si está activado LED de estado de Bluetooth , el LED azul parpadeará cuando se conecta.
Por Defecto: ON

LFD Level: Apagado/Bajo/Medio/Alto
Live Finger Detection para la detección de huellas dactilare falsas. Esta característica se puede utilizar para aplicaciones de mayor seguridad, cuando el usuario desea proteger contra las huellas dactilares falsas. Si el nivel es demasiado alto algunos usuarios registrados pueden tardar más tiempo para la autenticación de huellas dactilares .
Por Defecto: Off

Contraseña de inicio de sesión: 1-16 caracteres
Esta contraseña se utiliza para iniciar sesión en la aplicación B- UNIS a través del Smartphone
Por Defecto: 9999

Estado de la puerta #1: Deshabilitado/Normalmente Abierto/Normalmente Cerrado
Si un dispositivo de vigilancia (cerradura de la puerta) se conecta a la entrada de M0 en el BioB , este valor debe establecerse de acuerdo con los ajustes de los dispositivos externos . (NA o NC)
Por Defecto: Deshabilitado

Door Status #2: Deshabilitado/Normalmente abierto/Normalmente cerrado/Fuego Normalmente Abierto/Fuego Normalmente Cerrado.
Si un dispositivo de vigilancia se conecta a la entrada de la M1 en lel BioB , este valor debe establecerse de acuerdo con los ajustes de los dispositivos externos , si está conectado a un

sistema de fuego exterior y se detecta un incendio, el FMD10 abrirá la puerta.
Por Defecto: Deshabilitado

Tiempo Apertura de Puerta: 1-60 segundos
Este es el período de activación del relé. Si un relé está conectado a la salida de la cerradura, la cerradura se abre duante este período.
Por defecto: 3

Tecla de campana: 100-5000ms (0=deshabilitado)
Si la tecla de campana se utiliza para un timbre de la puerta , éste es el período en el que el botón de campana debe ser presionado para que suene. Si se establece 0 el toque de campana está desactivado .Default: 5000ms

Periodo de activación timbre: 0-60 segundos
Si se pulsa la tecla táctil de la campana, este es el período en el que la salida de sirena se activará. 0 = desactivado .
Por defecto : 1 segundo

Formato Tarjetas:Hexa Reversed, Hexa Normal, Decimal, Decimal_2
Cuando se escanea una tarjeta este ajuste determina el formato de codificación de la tarjeta.
Por Defecto: Hexa Reversed

Salida Wiegand : Deshabilitada/26 bit/34 bit
Si el FMD10 está conectado a un controlador externo utilizando las salidas Wiegand , este es el formato de la ID de usuario enviado al controlador externo mediante Wiegand .Nota: Sólo una autenticación correcta enviará la identificación del usuario mediante Wiegand.
Por Defecto: Deshabilitado

Wiegand SiteCode: 0-255 decimal
Si la salida Wiegand está habilitada, este es el código de identificación de 3 dígitos enviado antes que el identificador de usuario en la salida Wiegand (es decir, 2551234) esto es 255 y el ID de usuario = 1234.
Por Defecto: 0

Función de Bloqueo:

LOCAL = Establezca esta opción si se conecta el dispositivo de bloqueo en el dispositivo FMD10 . (Configuración predeterminada)
BLC015 / LC010 = Ajuste esta opción si la conexión de la cerradura a la LC010 o BLC015 .
485ID = (no compatible , no utilizar) Establezca esta opción y , a continuación, establezca ID 0-7 si se utiliza el 485A / B conectado a un controlador externo .

Nota: Para todos los dispositivos conectados externamente al FMD10 (cerraduras , monitoreo, Wiegand , etc) . Por favor vea la instalación FMD10 y Diagrama de cableado .
Al ajustar por BLC015 / LC010 , la salida de bloqueo y el Abrir en el FMD10 no funcionarán . En este caso, el bloqueo sólo se debe conectar a la BLC015 / LC010 .

Nivel 1:N : entradas válidas de 3-9

Esta opción representa el nivel de seguridad entre la huella digital capturada (por el sensor) , y las huellas dactilares almacenadas en el terminal. Este nivel representa el nivel terminal, no los usuarios individuales . Los valores posibles son de 3-9.Cuanto mayor sea el valor , mayor es el nivel de seguridad , lo que significa más comparaciones se realizan sobre los datos dactiloscópicos . Si las huellas dactilares de los usuarios están fallando durante la autenticación debe reducir este valor.

Nivel 1:1: entradas válidas de 1-9

Esta opción representa el nivel de seguridad correspondiente en el dispositivo entre la huella digital capturada (por el sensor) y la huella digital almacenada en la base de datos para ese usuario. Se utiliza este valor cuando se utiliza la tarjeta y autenticación de huellas digitales de este tipo,en lugar de comparar la huella digital capturada con todas las huellas digitales de base de datos , la huella digital única del usuario.Los valores posibles son 1-9 . Cuanto mayor sea el nivel de valor, mayor será el nivel de seguridad.

4. Cómo usar el Terminal

4.2. Autentificación

4.2.1. Autentificación Huellas Dactilares

Cuando pone el dedo en el sensor de huellas digitales , la luz del sensor se encenderá y el zumbador emitirá un sonido que indica un escaneo de huellas dactilares con éxito.No debe quitar el dedo hasta que se escuche el pitido. Si no hay usuarios registrados en el BioB , la luz de la huella dactilar no se enciende .

4.2.2. Autentificación de tarjeta

Pasar una tarjeta en el área de entrada de la tarjeta .

4.2.3. Autentificacion Correcta

Cuando se detecta una tarjeta o huella dactilar registrada en el BioB, puede activar una salida de relé por un período de tiempo programable para abrir la puerta. La señal acústica indicará una entrada correcta y el LED se iluminará de color verde para el período de apertura de la puerta.

4.2.4. Funcionamiento del timbre

Si se pulsa el botón del timbre para el período toque de campana , la salida de sirena se activará durante un período de tiempo programable (Período de activación del timbre) . El dispositivo de sonido emitirá un " ding- dong " y el LED parpadeará .
Si se presenta una huella dactilar o de la tarjeta durante el período de activación del timbre, la campana se apagará inmediatamente

Si una huella dactilar o tarjeta se utiliza, el botón de campana no aceptará ninguna pulsación del botón hasta que haya expirado el tiempo de apertura.