BioLite N2

GUÍA DE USUARIO DE

Versión 1.20

Español
ES 102.00.BLN2

suprema
SECURITY & BIOMETRICS

CONTENIDO

Instrucciones de Seguridad 4

Información de cumplimiento 4

Primeros Pasos 8

Componentes 8

Nombre y función de cada parte 9

Método correcto de ingreso de huellas dactilares 14

Instalación 16

Fijar el soporte y el producto 16

Conexión de la fuente de alimentación 19

Conexión de red 20

Conexión de entrada 21

Conexión del relé 22

Conectar como independiente 25

Conectar Secure I/O 2 26

Conexión Wiegand 28

Cómo Usar 29

Menú de Administrador 29

Usuario 29

Autenticación 31

Ajustes 37

Registros de eventos 43

Solución de Problemas 45

Verifique estos elementos antes de reportar una falla 45

Especificaciones del Producto 47

Credenciales 47

General 47

Capacidad 48

Interfaz 49

Eléctrico 49

Dimensiones y peso 50

Información Reglamentaria 51

Información de cumplimiento de la FCC 51

Información de IC 52

Declaración de conformidad de la UE (CE) 52

Apéndices 53

Descargos de responsabilidad 53

Aviso de derechos de autor 54

Licencia de código abierto 54

Instrucciones de Seguridad

Lea estas instrucciones de seguridad antes de usar el producto para evitar lesiones a usted y a otros y para prevenir daños a la propiedad.

El término «producto» en este manual se refiere al producto y a cualquier elemento suministrado con él.

Información de cumplimiento

Alerta

Se utiliza para indicar información de advertencia que, si se ignora durante el uso del producto, podría causar lesiones graves o la muerte.

Precaución

Se utiliza para indicar información de precaución que, si se ignora durante el uso del producto, puede provocar lesiones leves o daños al producto.

Información

Se utiliza para proporcionar notas o información adicional durante el uso del producto.

Nota

Se utiliza para proporcionar notas o información adicional durante el uso del producto.

⚠ Advertencia

Instalar

Tenga especial cuidado con el cableado incorrecto cuando use fuentes de alimentación de alta capacidad.

- Un cableado incorrecto puede provocar incendios graves, descargas eléctricas o daños al producto.

No permita que los usuarios instalen o reparen el producto de manera arbitraria.

- Puede causar incendios, descargas eléctricas o lesiones.
- No se proporcionará servicio de reparación gratuito si el producto resulta dañado debido a la instalación o reparación arbitraria por parte del usuario.

No instale el producto en lugares expuestos a la luz solar directa, humedad, polvo o hollín, ni donde pueda haber fugas de gas.

- Puede causar incendios o descargas eléctricas.

Al instalar el producto en exteriores, asegúrese de colocarlo en un área sombreada y bien ventilada.

No use un gabinete completamente sellado al instalar el producto en exteriores.

- La temperatura interna del gabinete puede aumentar debido a la luz solar directa, lo que puede provocar incendios, descargas eléctricas o daños al producto.

No instale el producto en lugares donde se genere calor, como cerca de calefactores.

- El sobrecalentamiento puede provocar incendios o descargas eléctricas.

No instale en lugares húmedos.

- La humedad puede provocar descargas eléctricas o daños al producto.

No instale en lugares con interferencia electromagnética.

- Puede provocar descargas eléctricas o daños al producto.

Uso

No permita que líquidos como agua, bebidas o productos químicos entren en el producto.

- Puede provocar incendios, descargas eléctricas o daños al producto.

No use adaptadores de corriente o enchufes dañados ni tomacorrientes flojos.

- Si las conexiones son inestables, pueden provocar incendios o descargas eléctricas.

No doble ni rompa en exceso el cable de alimentación.

- Puede causar incendios o descargas eléctricas.

⚠ Precaución

Instalar

Lea este manual detenidamente antes de instalar el producto para garantizar una instalación segura y correcta.

Al conectar cables de alimentación y conectores, asegúrese de apagar la alimentación de todos los dispositivos antes de cablear y conectar.

- Los dispositivos pueden funcionar incorrectamente.

Antes de conectar la alimentación al producto, revise nuevamente el manual para asegurarse de que el cableado sea correcto y luego conecte la alimentación.

No instale el producto en lugares expuestos directamente a la luz solar o ultravioleta.

- Puede provocar daños, mal funcionamiento, decoloración o deformación del producto.

No deje cables de alimentación en pasillos.

- Puede provocar lesiones corporales o daños al producto.

No instale cerca de objetos magnéticos fuertes como imanes, televisores, monitores CRT o altavoces.

- El dispositivo puede funcionar incorrectamente.

Al instalar el producto en una pared, no selle alrededor del dispositivo con silicona o materiales similares.

- El dispositivo puede funcionar incorrectamente.

Al instalar varios dispositivos, asegúrese de respetar la distancia mínima de separación.

- Puede afectar el rendimiento RF y BLE de otros dispositivos, provocando que funcionen incorrectamente.

Use un adaptador de corriente con aprobación IEC/EN 62368-1 y con capacidad superior al consumo de energía del dispositivo terminal. Se recomienda usar los adaptadores de corriente vendidos por Suprema.

- El uso de una fuente de alimentación inadecuada puede provocar el mal funcionamiento de los dispositivos.
- Consulte la sección Alimentación en las especificaciones del producto para conocer el consumo máximo de corriente.

Asegúrese de que el producto y Secure I/O 2, así como la cerradura eléctrica (dispositivo de bloqueo electrónico), utilicen fuentes de alimentación separadas.

- Los dispositivos pueden funcionar incorrectamente.

Se recomienda usar un gabinete cuando se instale en exteriores con exposición total.

- La disminución del rendimiento a prueba de agua y polvo puede provocar fallos.

Uso

No deje caer el producto ni lo someta a golpes.

- El dispositivo puede funcionar incorrectamente.

Asegure que no se interrumpa el suministro eléctrico durante las actualizaciones de firmware del producto.

- El dispositivo puede funcionar incorrectamente.

Administre la contraseña para que otros no la conozcan y cámbiela regularmente.

- Esto puede provocar acceso no autorizado.

No presione los botones (panel táctil) del producto con fuerza ni use herramientas puntiagudas para hacerlo.

- El dispositivo puede funcionar incorrectamente.

Use el producto dentro de -20 °C a 50 °C (BLN2-PAB: -10 °C a 50 °C) y guárdelo a temperaturas adecuadas, ni demasiado bajas ni demasiado altas.

- El dispositivo puede funcionar incorrectamente.

Tenga cuidado al limpiar el producto.

- Limpie suavemente la superficie del producto con un paño limpio y seco.
- Si va a desinfectar el producto, humedezca un paño limpio con la cantidad adecuada de alcohol desinfectante y limpie suavemente la superficie del producto. Use alcohol desinfectante que contenga 70-75 % de alcohol isopropílico y un paño suave, limpio y sin pelusa.
- No aplique desinfectante directamente sobre el producto.

No utilice el producto para fines distintos a su uso previsto.

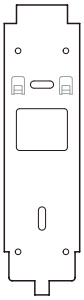
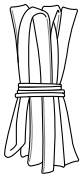
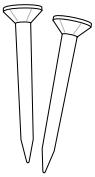
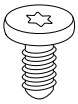
- El dispositivo puede funcionar incorrectamente.

> **Batería RTC**
>
> Reemplazar por baterías no autorizadas o de tipo incorrecto puede representar un riesgo de explosión. Deseche las baterías conforme a las normativas locales o internacionales sobre residuos.

Primeros Pasos

Proporciona procedimientos iniciales para empezar con el dispositivo.

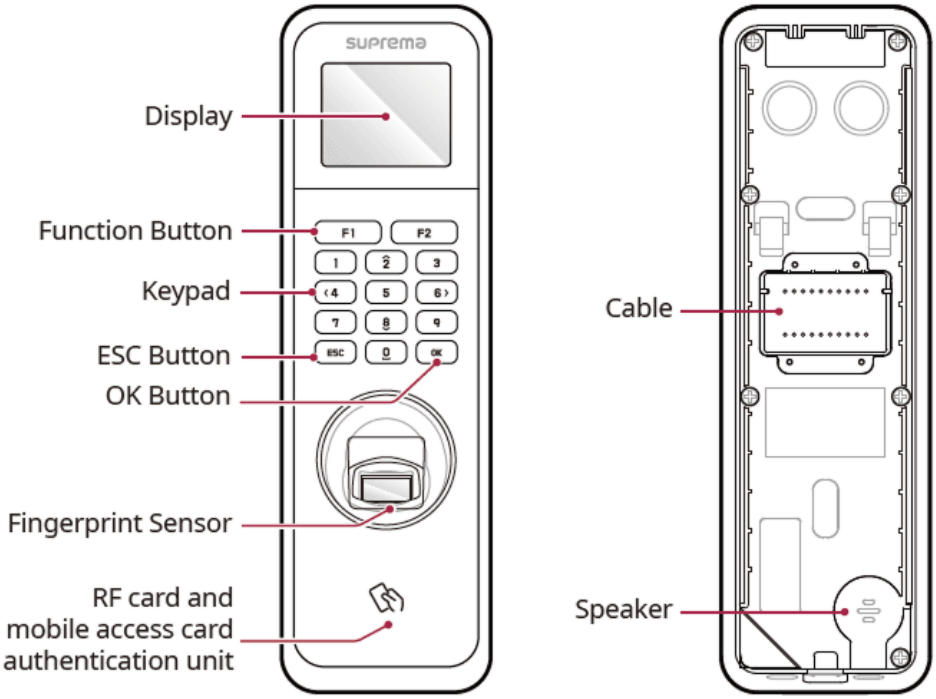
Componentes

		
BioLite N2	Soporte de pared	Tubo termorretráctil
		
Tornillos de fijación x2	Guía rápida	Guía de software de código abierto
		
Tornillo de fijación del soporte (en forma de estrella)	Resistencia de 120 Ω	Diodo

Información

- Los componentes pueden variar según el entorno de instalación.
- Al ensamblar el producto con el soporte, puedes usar el tornillo de fijación del soporte incluido (en forma de estrella) en lugar del tornillo de fijación del producto para aumentar la seguridad.

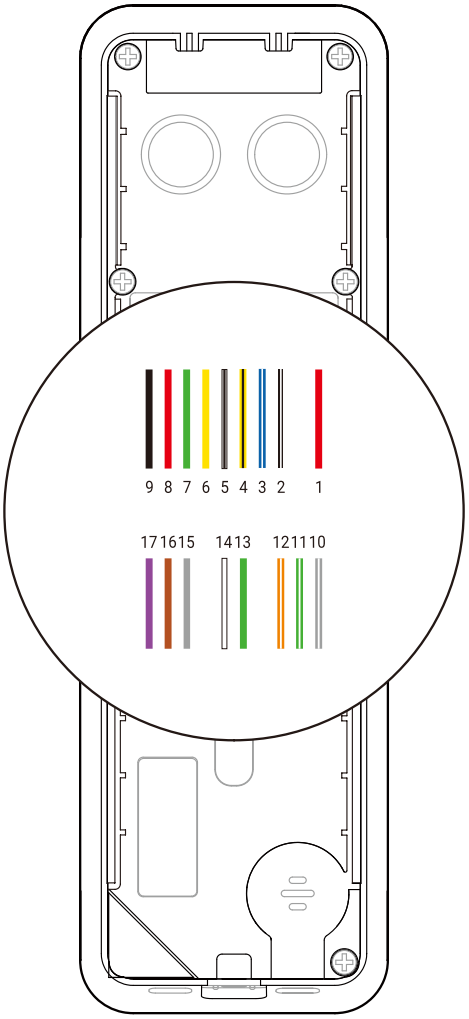
Nombre y función de cada parte



- **Pantalla**: Proporciona una interfaz de usuario para la operación.
- **Botón de funciones**: Se utiliza para la tecla de asistencia, la modificación de texto, etc.
- **Teclado**
  - **0-9**: Se utiliza para ingresar números o caracteres.
  - **2, 4, 6, 8**: Se utilizan para navegar al elemento deseado.
- **Botón OK**: Se utiliza para seleccionar el modo de asistencia y guardar los ajustes. Cuando el código de trabajo esté configurado, mantén presionado para cambiar el código de trabajo del usuario.
- **Botón ESC**: Se utiliza para abrir el menú, volver a la pantalla anterior y cancelar la entrada.
- **Unidad de reconocimiento de huella dactilar**: La parte que reconoce la huella dactilar para acceso.
- **Unidad de autenticación de tarjeta RF y tarjeta de acceso móvil**: parte para escanear una tarjeta RFID o una tarjeta de acceso móvil para la entrada.
- **Cable**

  Alimentación / RS-485 / Ethernet / Relé / Entrada/Salida Wiegand / Entrada
- **Altavoz**: Emite sonido.

Cable



Pin	Nombre	Color
1	PWR +VDC	Rojo
2	PWR GND	Negro (franja blanca)
3	485 TRXP	Azul (franja blanca)
4	485 TRXN	Amarillo (franja negra)
5	485 GND	Blanco (franja negra)
6	ENET RXN	Amarillo
7	ENET RXP	Verde
8	ENET TXN	Rojo
9	ENET TXP	Negro
10	RLY NO	Gris (franja blanca)
11	RLY COM	Verde (franja blanca)
12	RLY NC	Naranja (franja blanca)
13	WG D0	Verde
14	WG D1	Blanco
15	INPUT GND	Gris
16	INPUT1	Marrón
17	INPUT0	Morado

Configurar administrador maestro solo para modelos CE

La función **Master Admin** mejora los privilegios administrativos generales del dispositivo para aumentar la seguridad del dispositivo y evitar el acceso y los cambios de configuración no autorizados. Esta feature se aplica solo a **Productos CE** para la región de la UE, y se requiere el **enrollment del Master Administrator** en **Productos CE**. Solo el Master Administrator enrolled puede acceder al menú de administrador y cambiar los settings del dispositivo.

Información

- Esta feature es una policy obligatoria introducida para mejorar la seguridad de los **Productos CE** en la región de la UE, y no es compatible con **productos Global (No CE)**.
- El administrador maestro no puede eliminarse directamente y solo se eliminará durante **Factory Default**.

Política de soporte del Master Administrator Productos CE vs productos Global (No CE)

La feature **Master Admin** se activa solo en **Productos CE con una etiqueta que tiene la marca CE**.

Use la etiqueta adhesiva en el rótulo posterior para identificar **Productos CE** y **productos Global (No CE)**. La feature funciona de manera diferente, como se indica a continuación.

- **Productos CE**: marca CE presente
- **productos Global (No CE)**: marca CE ausente

Categoría	Productos CE	Productos Global (No CE)
Master Admin	Activado (no se puede desactivar)	No compatible
Admin 2-step Authentication	Obligatorio	No compatible
Longitud mínima del PIN	Al menos 8 dígitos	Al menos 4 dígitos

Cuando se conecta a BioStar X (o BioStar 2), el setting de Master Admin cambia según la compatibilidad del dispositivo, y la activación del menú de autenticación en dos pasos del administrador se sincroniza automáticamente.

Lógica de comportamiento durante la actualización del firmware

Cuando actualiza el firmware de un dispositivo existente, la compatibilidad con **Master Admin** y **Admin 2-step Authentication** puede variar según la combinación de la **versión anterior a la actualización** y la **versión objetivo**.

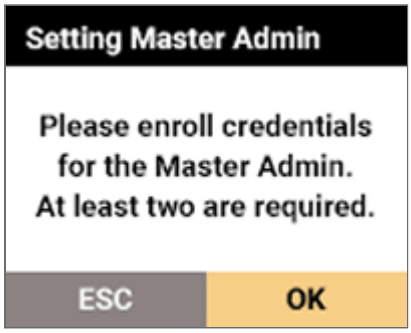
Contacte a Equipo de Soporte Técnico global de Suprema para obtener información detallada sobre la disponibilidad del soporte por versión.

Registrar Master Admin en un dispositivo nuevo

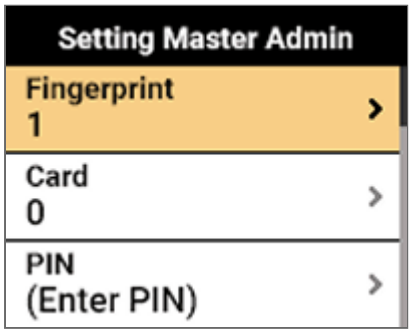
En un dispositivo nuevo para Productos CE, debe enrolar **Master Admin** desde el inicio. Si no lo enrola, el uso del dispositivo queda restringido.

> **Información**
>
> - En el primer arranque, aparece la pantalla de enrollment de **Master Admin**. Si no completa el enrollment, no puede pasar a la siguiente pantalla.
> - Aunque se conecte a BioStar X (o BioStar 2) y asigne un administrador para todo el dispositivo, debe inscribir **Master Admin** directamente en el dispositivo para usar todas las funciones.
> - Los dispositivos nuevos no pueden realizar degradaciones de firmware.

1. Cuando el dispositivo nuevo se inicie por primera vez, aparecerá la pantalla de registro de **Master Admin**. Presione **OK** para iniciar la inscripción.



2. Según la política de seguridad de la UE, **Master Admin** debe inscribir credenciales de al menos dos tipos. Seleccione e inscriba las dos credenciales deseadas.



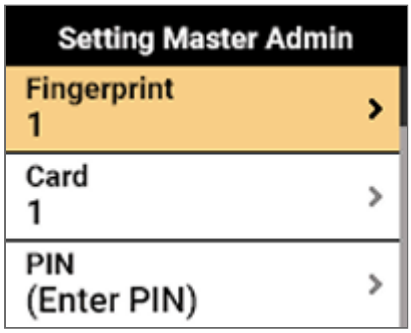
Las credenciales que se pueden inscribir para **Master Admin** son las siguientes.

Tipo de credencial	Número de inscripciones	Condiciones
Tarjeta	Hasta 4	Admite solo tipos CSN y Wiegand No se permite la inscripción duplicada dentro del mismo tipo
Rostro	Hasta 2	Inscriba solo en dispositivos con el mismo algoritmo
Fingerprint	Hasta 2	-

PIN	1	Al menos 8 dígitos (se aplica la normativa CE)

Condiciones de enrolamiento
- Debe enrolar al menos dos tipos de credenciales.
- Todas las credenciales compatibles con el dispositivo pueden utilizarse como medios de autenticación.

3. Después de inscribir dos o más tipos de credenciales, presione **OK** para completar la inscripción de **Master Admin**.



Información adicional

- **Cuando se enrola un PIN mediante el software BioStar**

  Los productos Global (No CE) que no admiten el Master Administrator pueden enrolar un PIN de al menos 4 dígitos directamente en el dispositivo. Sin embargo, al enrolar usuarios mediante BioStar X (o BioStar 2), las siguientes versiones requieren un PIN de al menos 8 dígitos.

  – BioStar 2 v2.9.11 o posterior

  – BioStar X v1.0.0 a v1.0.2

  Los usuarios enrolados con un PIN de 4 dígitos en las versiones anteriores no pueden asignarse como administradores del dispositivo.

- **Cambio manual de la clave hash del dispositivo**

  Al cambiar manualmente la clave hash del dispositivo, aparecerá un mensaje de advertencia que indicará que los PIN de Master Admin se eliminarán. Confirme el mensaje antes de continuar.

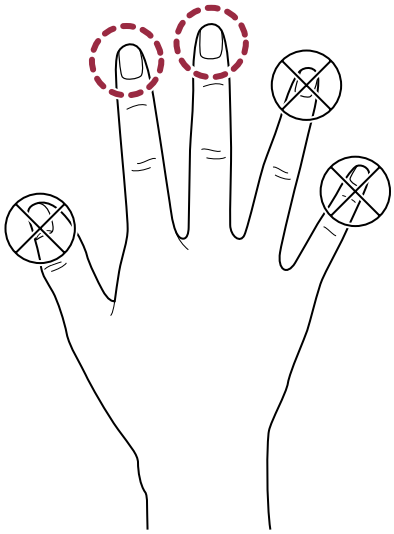
- **Restricción de transmisión de imágenes biométricas RS-485**

  Las imágenes de credenciales biométricas no se transmiten por comunicación RS-485, por lo que aparecen imágenes sustitutas al ver el rostro del Master Admin registrado en dispositivos esclavos.

Método correcto de ingreso de huellas dactilares

Registre la huella correctamente para mejorar la tasa de autenticación de huellas dactilares. Este producto puede autenticar huellas dactilares incluso si cambian el ángulo y la posición de ingreso de la huella. Registre la huella teniendo en cuenta los siguientes aspectos para mejorar la tasa de autenticación.

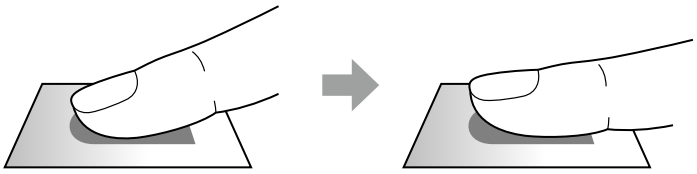
Selección de dedo para el ingreso de huella dactilar



- Para el caso de que la huella de un dedo específico no pueda utilizarse, por ejemplo, si el usuario sostiene una carga con una mano o se lesiona un dedo, se pueden registrar hasta 10 huellas dactilares por usuario.
- Si la huella de un usuario no se reconoce correctamente, registre el mismo dedo dos veces para mejorar la tasa de autenticación.
- Si un dedo tiene un corte o la huella está borrosa, seleccione otro dedo para la huella.
- Use el dedo índice o medio al escanear la huella. La tasa de autenticación puede reducirse si es difícil colocar otro dedo con precisión en el centro del sensor de huellas.

Método de registro de huellas dactilares

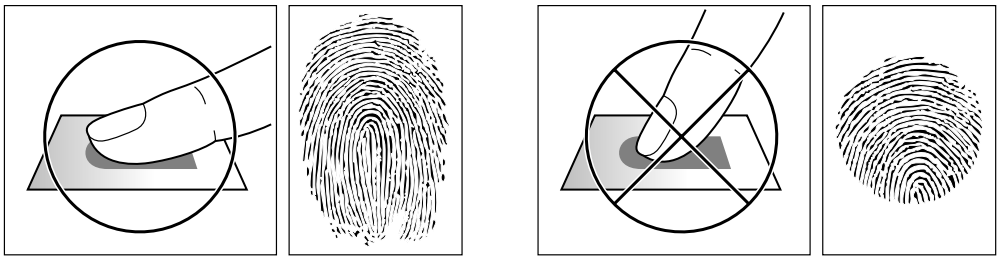
1. Cuando la pantalla muestre "Ingrese su huella", coloque el dedo que desea registrar en la unidad de reconocimiento de huellas y presiónelo suavemente para que la huella se autentique correctamente.



2. Cuando aparezca la pantalla de reingreso tras el beep, vuelva a escanear la huella del dedo registrado. (escanee dos veces la huella del dedo que va a registrar)

Precauciones para el registro de huellas dactilares

Cuando se reconoce una huella, se compara con la huella registrada inicialmente; por lo tanto, el registro inicial es el más importante. Tenga en cuenta los siguientes aspectos al registrar la huella.



- Coloque el dedo lo suficientemente profundo para que haga contacto completo con el sensor.
- Coloque el centro de la huella en el centro del sensor.
- Si un dedo tiene un corte o la huella está borrosa, seleccione otro dedo para la huella.
- Escanee la huella correctamente sin moverla, según las instrucciones de la pantalla.
- Si mantiene el dedo en posición vertical de modo que se reduzca el área de contacto con el sensor o cambia el ángulo del dedo, es posible que la autenticación de la huella no se realice.

Si la autenticación de huellas no funciona correctamente

Este producto puede autenticar huellas dactilares sin importar los cambios estacionales o el estado de los dedos. Sin embargo, la tasa de autenticación puede variar según el entorno externo o el método de ingreso de la huella. Si la autenticación de huellas no se realiza sin problemas, adopte las siguientes medidas.

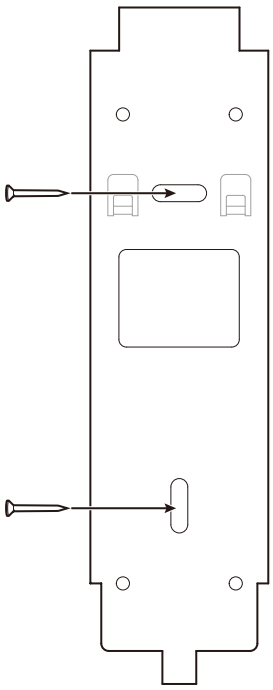
- Si el dedo está mojado o sudoroso, séquelo y luego escanee la huella.
- Si el dedo está demasiado seco, sople sobre la yema y luego escanee la huella.
- Si el dedo tiene un corte, registre la huella de otro dedo.
- Como la huella dactilar inscrita inicialmente con frecuencia no se introduce correctamente, vuelva a registrarla siguiendo las Precauciones para el registro de huellas dactilares.

Instalación

Ofrece los procedimientos completos de instalación y ejemplos de conexión necesarios para el dispositivo.

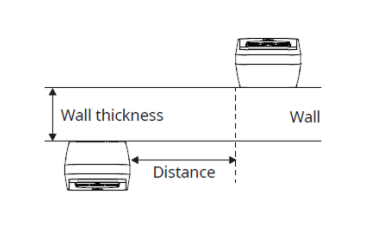
Fijar el soporte y el producto

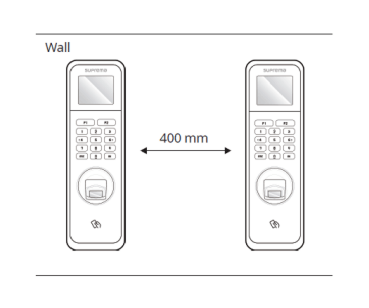
1. Asegura firmemente el soporte con los tornillos de fijación en el lugar donde se montará el producto.



Información

- Si instalas el producto en una pared de concreto, perfora un agujero, inserta un anclaje de PVC y sujétalo con un tornillo de fijación.
- Para evitar interferencias de RF, se debe mantener una distancia mínima de separación.

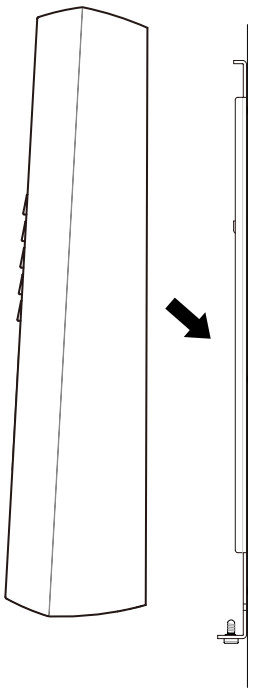




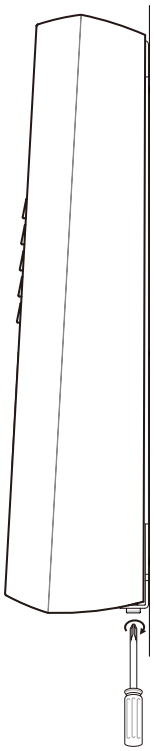
Espesor de pared	Distancia
100 mm	350 mm
120 mm	350 mm
150 mm	300 mm

- Al utilizar una credencial de acceso móvil, instala los dispositivos manteniendo una distancia mínima de 1 m entre ellos para evitar interferencias BLE.

2. Monta el producto en el soporte fijado.



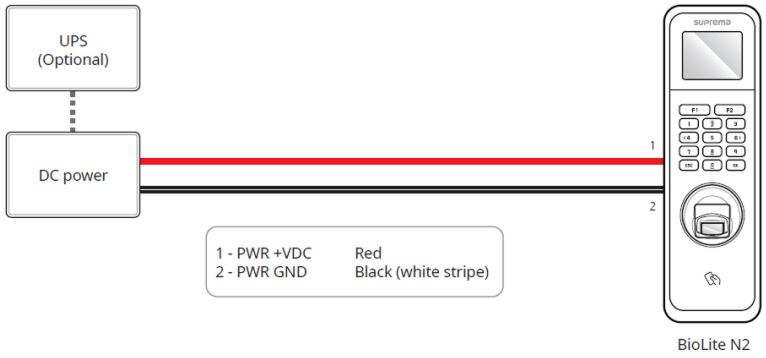
3. Gira los tornillos de fijación para ensamblar el producto con el soporte.



Información

Al ensamblar el producto con el soporte, puedes usar el tornillo de fijación del soporte incluido (en forma de estrella) en lugar del tornillo de fijación del producto para aumentar la seguridad.

Conexión de la fuente de alimentación



Precaución

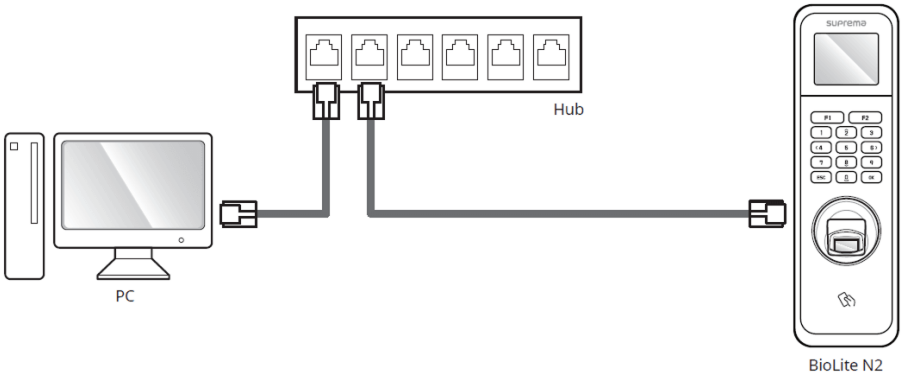
- Use un adaptador de alimentación aprobado por IEC/EN 62368-1 que admita un consumo de energía mayor que el del producto. Si desea conectar y usar otro dispositivo al adaptador de alimentación, utilice un adaptador con una capacidad de corriente igual o mayor que el consumo total requerido por el terminal y el otro dispositivo.
  - Consulte la sección Alimentación en las especificaciones del producto para conocer el consumo máximo de corriente.
- Use una fuente de alimentación independiente para Secure I/O 2, la cerradura eléctrica y el producto, respectivamente. Si conecta y usa la misma fuente de alimentación para estos dispositivos, estos pueden funcionar incorrectamente.
- NO extienda la longitud del cable de alimentación al usar el adaptador de alimentación.

Conexión de red

TCP/IP

Conexión LAN (conexión a un concentrador)

Conéctese a un concentrador usando un cable CAT-5 estándar o superior.



Conexión LAN (conexión directa a una PC)

Este producto admite MDI/MDIX automático, por lo que puede conectarse directamente a una PC mediante un cable cruzado o un cable CAT-5 recto estándar o superior.



Puertos y servicios de red

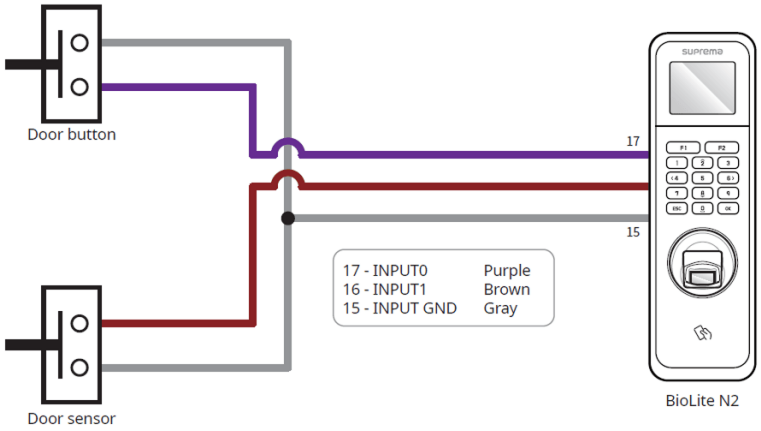
Este dispositivo usa los siguientes puertos para la comunicación de red y el funcionamiento estable del servicio.

Protocolo	Servicio
TCP	Se utiliza para los servicios de comunicación entre el servidor y el dispositivo, así como para el servicio de cambio de estado operativo del dispositivo.
UDP	Se usa para el servicio de detección del dispositivo, que permite buscar dispositivos en la red.

Información

Estos puertos se usan para proporcionar las funciones normales de red del producto. Al configurar las reglas del firewall o los ajustes de seguridad de red, permita el uso de estos puertos.

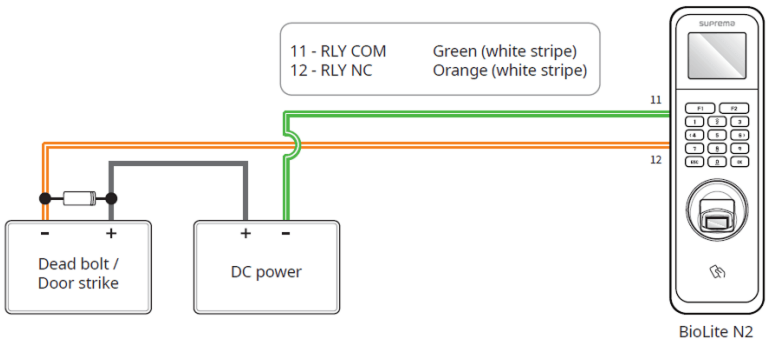
Conexión de entrada



Conexión del relé

Cerradura fail safe

Para utilizar la cerradura Fail Safe, conecte el relé N/C como se muestra en la figura a continuación. Normalmente circula corriente a través del relé de la cerradura Fail Safe. Cuando se activa el relé y se bloquea el flujo de corriente, la puerta se abrirá. Si se corta la alimentación del producto debido a un fallo de energía o a un factor externo, la puerta se abrirá.



Precaución

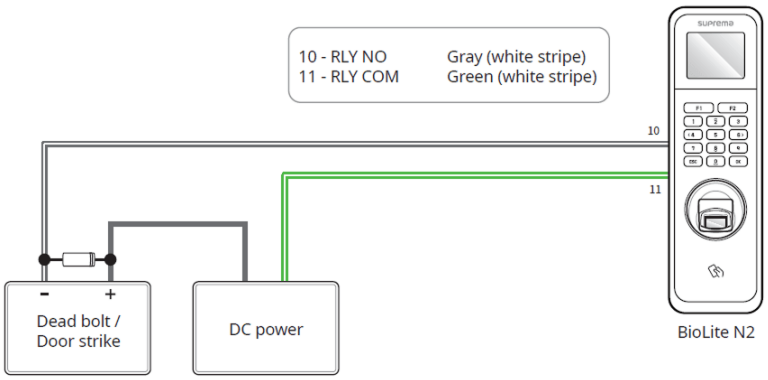
- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes de Suprema contienen relés internos que pueden bloquear/desbloquear puertas directamente sin controladores externos para mayor comodidad. Sin embargo, para aplicaciones de control de acceso que requieren seguridad, NO se recomienda utilizar el relé interno de un lector a fin de evitar manipulaciones que puedan desbloquear la puerta. Para estas aplicaciones, se recomienda encarecidamente usar una unidad de relé independiente para el control de la cerradura, como Secure I/O 2, DM-20 o CoreStation de Suprema, instaladas en el lado seguro de la puerta.

Información

Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

Cerradura fail secure

Conecte el relé N/O como se muestra en la figura para usar la cerradura fail secure. Normalmente no circula corriente a través del relé para la cerradura Fail Secure. Cuando el relé activa el flujo de corriente, la puerta se abrirá. Si el suministro eléctrico del producto se interrumpe debido a un corte de energía o a un factor externo, la puerta se bloqueará.



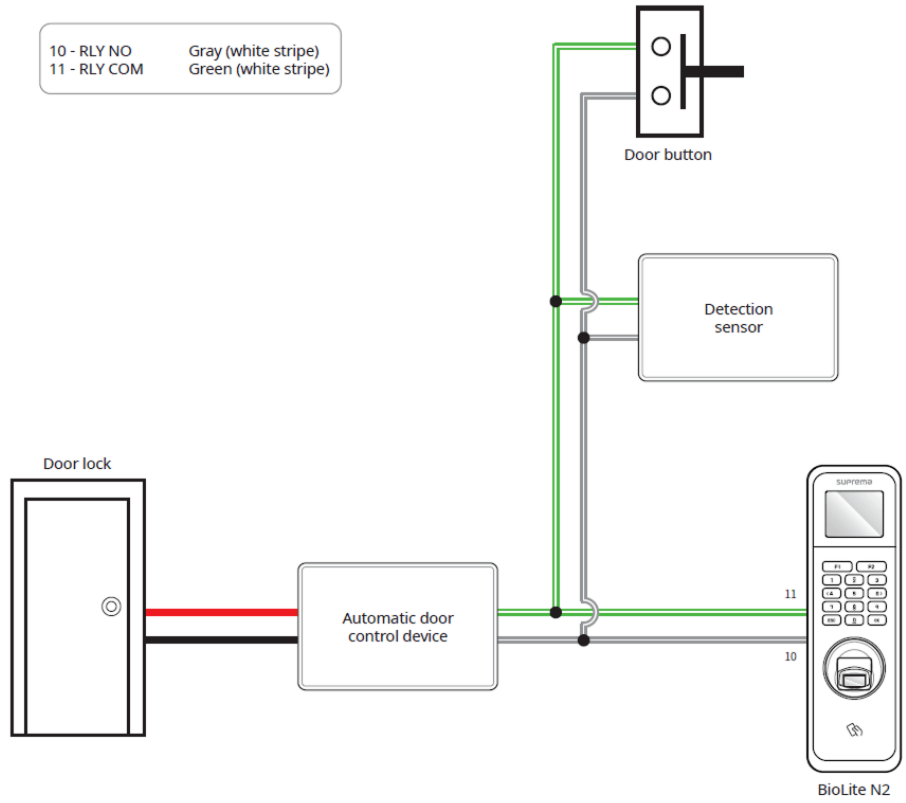
Precaución

- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes de Suprema contienen relés internos que pueden bloquear/desbloquear puertas directamente sin controladores externos para mayor comodidad. Sin embargo, para aplicaciones de control de acceso que requieren seguridad, NO se recomienda utilizar el relé interno de un lector a fin de evitar manipulaciones que puedan desbloquear la puerta. Para estas aplicaciones, se recomienda encarecidamente usar una unidad de relé independiente para el control de la cerradura, como Secure I/O 2, DM-20 o CoreStation de Suprema, instaladas en el lado seguro de la puerta.

Información

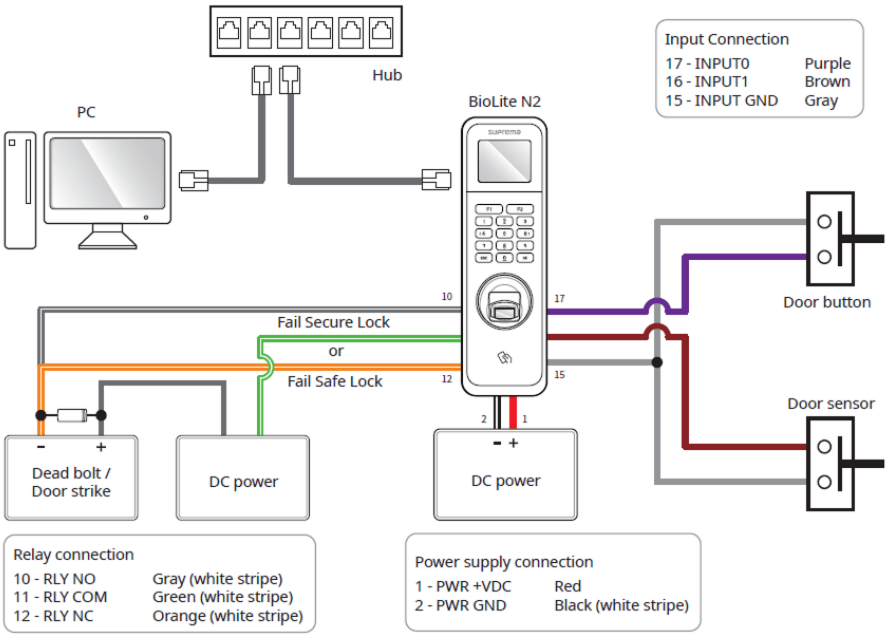
Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

Conexión de puerta automática



Conectar como independiente

El producto puede conectarse directamente a la cerradura, el botón y el sensor de puerta sin necesidad de conectar un dispositivo de E/S adicional.



Precaución

Los lectores inteligentes independientes de Suprema contienen relés internos que pueden bloquear/desbloquear puertas directamente sin controladores externos para mayor comodidad. Sin embargo, para aplicaciones de control de acceso que requieren seguridad, NO se recomienda utilizar el relé interno de un lector a fin de evitar manipulaciones que puedan desbloquear la puerta. Para estas aplicaciones, se recomienda encarecidamente usar una unidad de relé independiente para el control de la cerradura, como Secure I/O 2, DM-20 o CoreStation de Suprema, instaladas en el lado seguro de la puerta.

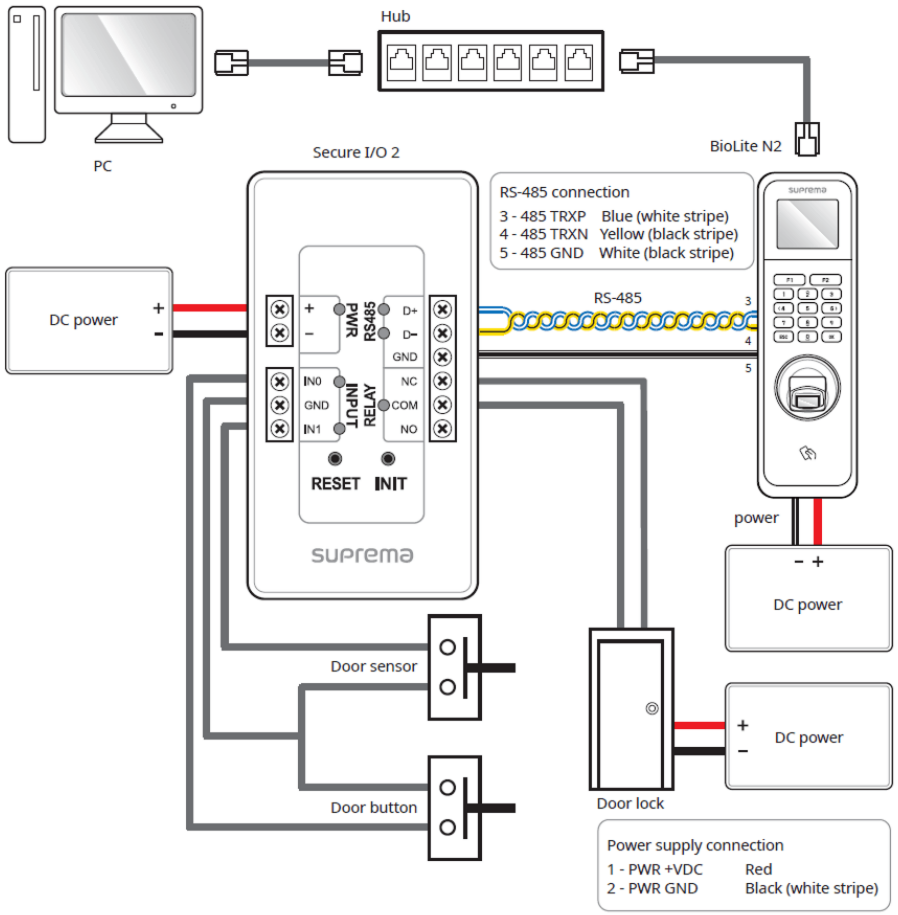
Información

- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- Si se conecta XPass o XPass 2 al dispositivo maestro, solo se puede usar la autenticación con tarjeta.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.
- Conecte hasta 31 dispositivos esclavos a un dispositivo maestro. El ancho de banda de RS-485 permite conectar hasta 7 dispositivos de autenticación por huella.
- Para más información, comuníquese con el Equipo de soporte técnico de Suprema.

Conectar Secure I/O 2

Secure I/O 2 es un dispositivo de E/S que se puede conectar al producto con el cable RS-485. La seguridad puede mantenerse incluso si se pierde la conexión entre el producto y Secure I/O 2 o si el suministro de energía al producto se interrumpe debido a factores externos.

- Utilice un par trenzado AWG24 con una longitud máxima de 1.2 km para el cable RS-485.
- Se recomienda usar cables RS-485 con una impedancia característica de 120 Ω.
- Si se conecta mediante una cadena en serie RS-485, conecte la resistencia de terminación (120 Ω) en ambos extremos de la conexión en cadena. Si se conecta en la línea media, el nivel de señal se reducirá y el rendimiento de comunicación se verá afectado. Asegúrese de conectarlas en ambos extremos de la conexión en cadena.

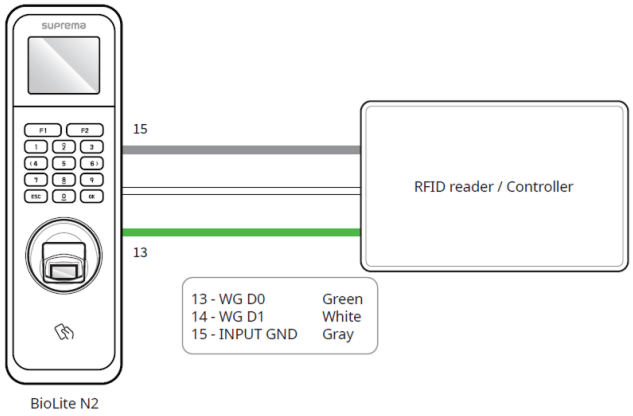


Información

- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- Si se conecta XPass o XPass 2 al dispositivo maestro, solo se puede usar la autenticación con tarjeta.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.
- Conecte hasta 31 dispositivos esclavos a un dispositivo maestro. El ancho de banda de RS-485 permite conectar hasta 7 dispositivos de autenticación por huella.
- Para más información, comuníquese con el Equipo de soporte técnico de Suprema.

Conexión Wiegand

Use como dispositivo de entrada o salida Wiegand.



Cómo Usar

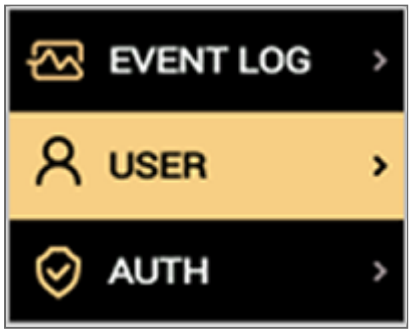
Proporciona orientación sobre cómo utilizar las funciones principales del dispositivo de manera efectiva.

Menú de Administrador

Proporciona orientación sobre los menús principales y las funciones accesibles con privilegios de administrador.

Menú completo

1. Pulsa **ESC** y autentícate como administrador.
2. Selecciona el menú deseado.



> **Información**
> Si no se especifica ningún administrador, presiona **ESC** para mostrar la pantalla de menú.

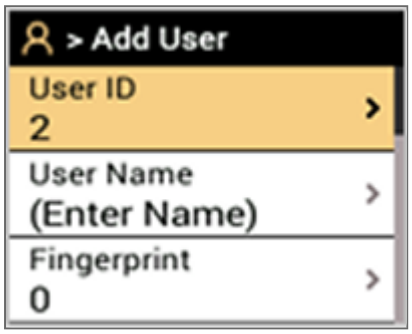
Usuario

Describe cómo registrar, editar, eliminar y gestionar usuarios.

Registrar información de usuario

Registre información de usuario que incluya datos de autenticación biométrica.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **USER** → **Add User** y luego presione **6**.



3. Seleccione el elemento deseado y presione **4** o **6** para configurarlo. Presione **OK** para registrar la información del usuario.

   - **ID**: Ingrese un número entre 1 y 4294967294 para registrar un ID de usuario. Si **User ID Type** está configurado en **Alphanumeric**, puede usar una combinación de caracteres alfanuméricos y los símbolos `_` `-` como ID, con un máximo de 32 caracteres.
   - **Name**: Puede ingresar un nombre de usuario usando los botones numéricos y de función.
   - **Fingerprint**: Inscriba una huella digital para la autenticación del usuario. Después de escanear la huella digital del dedo que se va a inscribir, vuelva a escanear la huella del mismo dedo. Seleccione la huella digital que desea eliminar y presione **4** para eliminarla, o presione **6** para escanearla nuevamente. Para agregar más huellas digitales, seleccione **+ Add Finger** y luego presione **6**.
   - **Card**: Inscriba una tarjeta para la autenticación del usuario. Escanee la tarjeta que se asignará al usuario en la unidad de reconocimiento de tarjetas RF.
   - **PIN**: Ingrese el PIN que desea usar. Después de ingresar el PIN deseado, ingréselo nuevamente para confirmación. Para evitar filtraciones, ingrese un PIN de 4 a 16 dígitos.

     > **Información**
     > Al usar la función **Master Admin**, ingrese un número de al menos 8 dígitos.

   - **Operator Level**: Seleccione los permisos que desea asignar al usuario.

     > **Información**
     > Los menús disponibles varían según el nivel de usuario establecido.
     > – **Normal User**: Este es un nivel de usuario regular y no puede acceder al menú.
     > – **Administrator**: Puede usar todos los menús.
     > – **Configuration**: Puede usar los menús **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK**, **EVENT LOG**.
     > – **User Management**: Puede usar los menús **USER**, **EVENT LOG**.

   - **Start Date**: Configure la fecha de inicio de uso de la cuenta de usuario.
   - **Expiration Date**: Configure la fecha de finalización de uso de la cuenta de usuario.
   - **1:1 Security Level**: Puede establecer el nivel de seguridad para la autenticación 1:1.
   - **Duress**: Puede seleccionar el número de huella digital que se utilizará como huella digital de amenaza. Debe inscribir al menos 2 huellas digitales para usar esta función.
   - **Private Auth Mode**: Puede cambiar el método de autenticación para cada usuario.

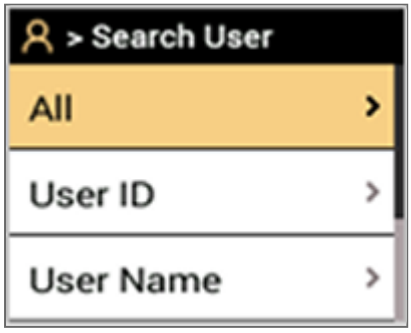
4. Pulsa **OK** para guardar la configuración.

Modificar información de usuario

El gestor de usuarios o el administrador pueden modificar la información de usuario registrada. Agregue la huella digital o la tarjeta del usuario y modifique el PIN y los permisos.

1. Pulsa **ESC** y autentícate como administrador.

2. Seleccione **USER** → **Search User** y luego presione **6**.
3. Seleccione los términos de búsqueda. Puede buscar usuarios usando **All**, **ID**, **Name**, **Fingerprint**, **Card**.



4. Seleccione al usuario que desea modificar y luego presione **6**. Consulte Registrar información de usuario para modificar la información.
   - Para eliminar un usuario, seleccione **4** y luego presione **OK**.

> **Información**
> **Access Group** se puede registrar en BioStar X. Para obtener información detallada sobre cómo registrar un Grupo de Acceso, consulte la Guía del Administrador de BioStar X.

Eliminar todos los usuarios

Elimine todos los usuarios registrados a la vez.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **USER** → **Delete All Users** y luego presione **6**.
3. Presione **OK** para eliminar a todos los usuarios registrados.

Ver uso de usuarios

Vea de un vistazo la cantidad de usuarios, huellas digitales y tarjetas inscritas.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **USER** → **User Usage** y luego presione **6**. La información de uso de usuarios aparece.

Autenticación

Describe los métodos de autenticación compatibles y los procedimientos de autenticación.

Modo de autenticación

Configura el modo de autenticación. Combina **Fingerprint**, **PIN**, **Card** y **ID** para el modo de autenticación y establece horarios para cada modo de autenticación.

Modo de autenticación por huella

Define horarios para cada método de autenticación que use huellas.

1. Pulsa **ESC** y autentícate como administrador.
2. Después de seleccionar **AUTHENTICATION** → **Auth Mode** → **Fingerprint Mode**, pulsa **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para configurar el horario.



   - : Este modo utiliza solo huellas.
   - \+ : Este modo autentica con una huella y luego con la introducción de un PIN.
4. Pulsa **OK** para guardar la configuración.

> **Información**
>
> - Configura **Schedule** en BioStar X. Sin horarios definidos, solo se pueden seleccionar **Never** y **Always**.
> - Para más información sobre la configuración de **Schedule**, consulte la Guía del administrador de BioStar X.

Modo de autenticación por tarjeta

Define horarios para cada método de autenticación que use tarjetas.

1. Pulsa **ESC** y autentícate como administrador.
2. Después de seleccionar **AUTHENTICATION** → **Auth Mode** → **Card Mode**, pulsa **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para configurar el horario.



   - : Este modo utiliza solo tarjetas.

- + : Este modo autentica con una tarjeta seguida de autenticación por huella.
- + : Este modo utiliza una tarjeta para autenticarse y luego ingresa un PIN.
- + / : Este modo autentica con una tarjeta seguida de huella o ingreso de PIN.
- + + : Este modo utiliza una tarjeta seguida tanto de autenticación por huella como de ingreso de PIN.

4. Pulsa **OK** para guardar la configuración.

> **Información**
>
> - Configura **Schedule** en BioStar X. Sin horarios definidos, solo se pueden seleccionar **Never** y **Always**.
> - Para más información sobre la configuración de **Schedule**, consulte la Guía del administrador de BioStar X.

Modo de autenticación por ID

Define horarios para cada método de autenticación que use ID.

1. Pulsa **ESC** y autentícate como administrador.
2. Después de seleccionar **AUTHENTICATION** → **Auth Mode** → **ID Mode**, pulsa **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para configurar el horario.



- + : Este modo autentica con un ID seguido de huella.
- + : Este modo utiliza un ID seguido del ingreso de un PIN.
- + / : Este modo utiliza un ID seguido de autenticación por huella o ingreso de PIN.
- + + : Este modo utiliza un ID seguido tanto de autenticación por huella como de ingreso de PIN.

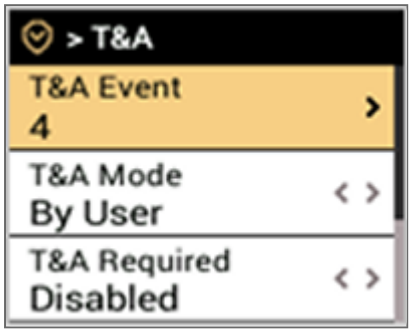
4. Pulsa **OK** para guardar la configuración.

> **Información**
>
> - Configura **Schedule** en BioStar X. Sin horarios definidos, solo se pueden seleccionar **Never** y **Always**.
> - Para más información sobre la configuración de **Schedule**, consulte la Guía del administrador de BioStar X.

Modo de asistencia

Configura cómo registrar el modo T&A.

1. Pulsa **ESC** y autentícate como administrador.
2. Selecciona **AUTHENTICATION** → **T&A** y luego pulsa **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para configurar el horario.



   - **T&A Event**: Permite revisar los eventos de asistencia.
   - **T&A Mode**: Configura cómo usar el modo de asistencia.
   - **T&A Required**: Configure para que el usuario tenga que seleccionar un evento de T&A al autenticarse. Al configurar **Enabled**, se exige seleccionar un evento de tiempo y asistencia durante la autenticación.
   - **T&A Fixed**: Configura el uso únicamente de eventos de tiempo y asistencia seleccionados por un administrador. Disponible cuando **T&A Mode** está configurado en **Fixed**.
   - **Job Code**: Configure si se usará el código de puesto.
4. Pulsa **OK** para guardar la configuración.

> **Información**
>
> Configura **Job Code** en **Enabled** para cambiar el código de acción del usuario. Mantén presionado **OK** y luego autentícate para seleccionar el código de trabajo deseado.

Ajustes de huella

Cambia los ajustes de autenticación por huella digital.

1. Pulsa **ESC** y autentícate como administrador.
2. Después de seleccionar **AUTHENTICATION** → **Fingerprint**, pulsa **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para configurar el horario.



- **Security Level**: Configura el nivel de seguridad para la autenticación 1:N.
- **Matching Timeout**: Configura el tiempo de espera para la correspondencia de huellas. Si la autenticación no se completa dentro del tiempo especificado, fallará.
- **View Image**: Se puede ver la imagen original de la huella escaneada.
- **Sensor Sensitivity**: Configura la sensibilidad del sensor de reconocimiento de huellas. Establece la sensibilidad más alta para obtener información de huella dactilar precisa.
- **Live Finger Detection**: Configura el nivel de detección de huellas falsas. Niveles más altos de detección de huellas falsas pueden aumentar las tasas de rechazo de las huellas reales.
- **1:N Fast Mode**: Configura la velocidad de la autenticación por huella. Al seleccionar **Auto**, la velocidad de autenticación se ajusta según el total de plantillas de huellas almacenadas en el dispositivo.
- **Template Format**: Configura el formato de plantilla de huella. **SUPREMA** está configurado por defecto. Al cambiar el formato de la plantilla, las huellas digitales guardadas anteriormente quedarán inutilizables, así que tenga cuidado al modificarlo.

  > **Información**
  > Elimina toda la información de huellas dactilares de los usuarios y luego cambia el formato de la plantilla. Si hay información de huellas dactilares registrada, no es posible cambiar el formato de la plantilla.

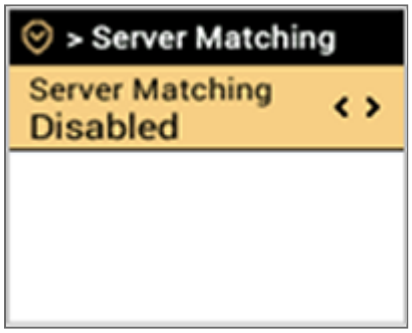
- **Sensor Mode**: Configura en **Auto On** para encender el sensor de huella cuando detecte el dedo del usuario. Al configurarse en **Always On**, el sensor permanece encendido aunque no se estén escaneando huellas.
- **Advanced Enrollment**: Evalúa la calidad de las huellas escaneadas para guardar información de alta calidad. Habilite la notificación para avisar al usuario cuando la calidad de la huella digital sea baja, ayudándole a escanearla correctamente.
- **Duplicate Check**: Verifica huellas duplicadas durante el enrolamiento.

4. Pulsa **OK** para guardar la configuración.

Autenticación en servidor

Configura la autenticación en servidor. Cuando se utiliza la autenticación en servidor, la autenticación se realiza en BioStar X sin autenticación en el dispositivo. Se puede usar cuando el dispositivo tiene demasiada información de usuarios o cuando el dispositivo está instalado en exteriores.

1. Pulsa **ESC** y autentícate como administrador.
2. Después de seleccionar **AUTHENTICATION** → **Server Matching**, pulsa **6**.



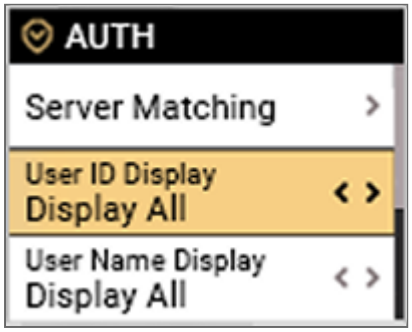
3. Pulsa **4** o **6** para cambiar los ajustes.
4. Pulsa **OK** para guardar la configuración.

> **Información**
>
> - **Server Matching** solo puede usar **Fingerprint**, **Card** y **ID**.
> - Si usa **Server Matching**, habilite la coincidencia con el servidor tanto en el dispositivo como en BioStar X. Para obtener información detallada sobre la configuración de la coincidencia con servidor en BioStar X, consulte la Guía del administrador de BioStar X.

Opciones de visualización del resultado de autenticación

Configura la opción de visualización del resultado de autenticación.

1. Pulsa **ESC** y autentícate como administrador.
2. Después de seleccionar **AUTHENTICATION**, pulsa **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para cambiar los ajustes.



- **User ID Display**: Seleccione cómo se muestra el ID de usuario en la pantalla de resultados de autenticación del dispositivo.
  - **Display All**: Muestra todos los ID de usuario.
  - **Mask All but First Letter**: Muestra solo la primera letra del ID de usuario.
  - **Hide All**: No mostrar el ID de usuario.
- **User Name Display**: Seleccione cómo se muestra el nombre del usuario en la pantalla de resultados de autenticación del dispositivo.
  - **Display All**: Muestra todos los nombres de usuario.
  -

Mask All but First Letter: Muestra solo la primera letra del nombre del usuario.

– **Hide All**: No mostrar el nombre del usuario.

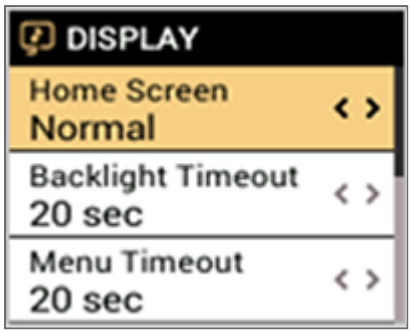
Ajustes

Proporciona instrucciones para configurar los ajustes del sistema y del dispositivo.

Pantalla y sonido

Cambie los ajustes de pantalla y sonido del dispositivo.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DISPLAY & SOUND** y presione **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para configurar el horario.



- **Home Screen**: Permite elegir los elementos que se mostrarán en el fondo de la pantalla de inicio.
- **Backlight Timeout**: Configure el tiempo (s) para apagar la iluminación de la pantalla.
- **Menu Timeout**: Configure el tiempo (s) para que la pantalla de menú desaparezca automáticamente. Si no se pulsa ningún botón durante el tiempo establecido, la pantalla regresará a la pantalla de inicio.
- **Message Timeout**: Configure el tiempo (s) para que un mensaje de configuración completada o de notificación desaparezca automáticamente.
- **Language**: Permite seleccionar el idioma que se mostrará en la pantalla.
- **Voice Instruction**: Permite usar guía por voz en lugar de tonos de notificación.
- **Volume**: Configure el volumen.

4. Pulsa **OK** para guardar la configuración.

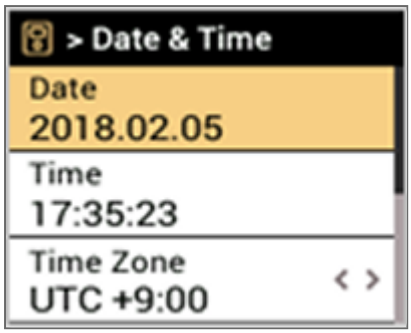
Dispositivo

Fecha y hora

Configura la fecha y la hora. Configura la fecha y la hora con precisión para recopilar datos de registro precisos.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Date & Time** y presione **6**.

3. Selecciona el elemento deseado y pulsa **4** o **6** para configurar el horario.



   - **Date**: Verifique la fecha actual. Para modificarla manualmente, desactive **Time Sync**.
   - **Time**: Verifique la hora actual. Para modificarla manualmente, desactive **Time Sync**.
   - **Time Zone**: Ajuste la referencia horaria de la ubicación actual.
   - **Time Sync**: Sincronice el servidor y la hora. Si desea sincronizar el servidor y la hora, habilite **Time Sync**.
   - **Date Format**: Configure el formato de fecha. Seleccione **YYYY/MM/DD**, **MM/DD/YYYY** y **DD/MM/YYYY**.
   - **Time Format**: Configure el formato de hora. Seleccione **24-Hour** y **AM/PM**.

4. Pulsa **OK** para guardar la configuración.

Horario de verano

Aplica el horario de verano para usar el dispositivo. Configura correctamente la hora de inicio y fin.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Daylight Saving Time** y presione **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para cambiar los ajustes.
   - **Name**: Establece el nombre del horario de verano.
   - **Start Month** / **Start Week** / **Start Day** / **Start Time**: Configure los detalles sobre cuándo comienza el horario de verano.
   - **End Month** / **End Week** / **End Day** / **End Time**: Configure los detalles sobre cuándo termina el horario de verano.
4. Pulsa **OK** para guardar la configuración.

Relé

Configure los puertos de entrada de **Open Time** y **Exit Button** en el dispositivo. Útil cuando se utiliza como dispositivo independiente.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Relay** y presione **6**.
   - **Relay**: Configure si el relé está habilitado. Habilitar el ajuste de relé permite configurar **Open Time** y **Exit Button**.
   - **Open Time**: Establece la duración que la puerta permanece abierta cuando se ha realizado la autenticación de usuario estándar.

- **Exit Button**: Selecciona el puerto de entrada conectado al botón de salida.
- **Switch**: Seleccione el tipo de interruptor (**N/O** o **N/C**) para el puerto de entrada del botón de salida.

3. Pulsa **OK** para guardar la configuración.

Información del dispositivo

Consulta el nombre del modelo, el ID del dispositivo, el número de serie, la versión del dispositivo y del firmware, el kernel y la dirección MAC.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Device Info** y presione **6**. Verifica la información de **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC**.
3. Presione **ESC** para regresar a la pantalla anterior.

Uso de memoria

Consulta el estado de uso de la memoria.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Memory Usage** y presione **6**. Consulta el estado de uso de memoria del dispositivo.
3. Presione **ESC** para regresar a la pantalla anterior.

Sabotaje

Configura si se utiliza el tamper de seguridad. Cuando el tamper está activado, establece la eliminación de todos los usuarios, todos los registros y la clave de seguridad.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Secure Tamper** y presione **4** o **6** para cambiar la configuración.
3. Pulsa **OK** para guardar la configuración.

Reiniciar dispositivo

Reinicia el dispositivo.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Restart Device** y presione **6**.
3. Presione **OK** para reiniciar el dispositivo. Pulsa **ESC** para cancelar.

Restaurar valores predeterminados

Los ajustes del dispositivo, los ajustes de red y los niveles de operador se restablecerán.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Restore Default** y presione **6**.

- **Reset All Settings**: Inicializa todos los ajustes guardados en el dispositivo. Presione **OK** para inicializar todas las configuraciones del dispositivo. Presione **ESC** para regresar a la pantalla anterior.
- **Quick Reset**: Inicializa todos los ajustes excepto los de red. Presione **OK** para inicializar todas las configuraciones excepto las de red. Presione **ESC** para regresar a la pantalla anterior.
- **Factory Default**: Elimina toda la información guardada en el dispositivo y el certificado raíz, y restaura los ajustes predeterminados.
- **Delete the Root Certificate**: Elimina el certificado raíz guardado en el dispositivo.

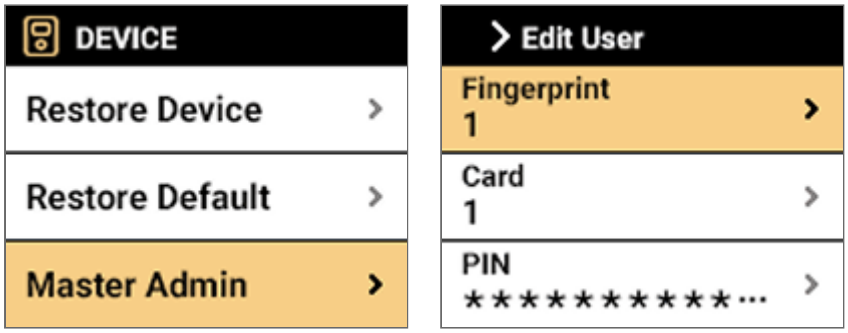
3. Si continúas con **Restore Default**, el dispositivo se reiniciará.

> **Información**
>
> - Al restablecer, el nivel de operador también se restablecerá. Después de restablecer, vuelve a configurar el nivel de operador.
> - El ajuste de idioma no cambiará después de restablecer.
> - El menú **Factory Default** puede utilizarse cuando el certificado raíz está guardado en el dispositivo.
> - El menú **Delete the Root Certificate** puede utilizarse solo cuando el certificado raíz está guardado en el dispositivo y se ha designado un administrador.

Administrador principal productos CE

Cambie el método de autenticación del administrador maestro.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Master Admin**.
3. Configure los métodos de autenticación deseados.



> **Información**
>
> - Debe enrolar al menos dos tipos de credenciales.
> - Disponible solo en dispositivos nuevos con firmware v1.7.0 o posterior.

Autenticación en dos pasos del administrador productos CE

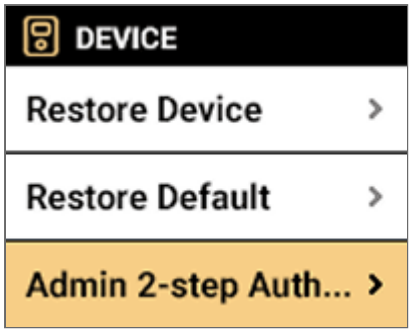
Un producto CE actualizado mediante firmware no ofrece settings de **Master Admin**, pero puede usar la opción **Admin**

2-step Authentication para mejorar los privilegios generales del administrador y la seguridad del dispositivo.

Información

- **Admin 2-step Authentication** se puede activar solo si todos los administradores enrolled tienen al menos dos tipos de credenciales.
  - El PIN no se puede usar como credencial independiente, por lo que la combinación ID + PIN no es compatible.
- El dispositivo actualizado mediante firmware no puede degradarse a una versión inferior después de la actualización.

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **Admin 2-step Authentication**.

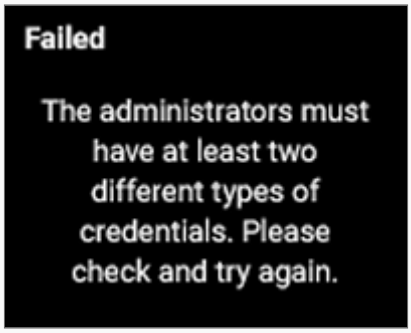


Información

Si no hay dos tipos de credenciales enroladas para todos los administradores, la activación falla y se muestra un mensaje de error.

Enrole dos tipos de credenciales para todos los administradores e inténtelo nuevamente.

- El PIN no se puede usar como credencial independiente, por lo que la combinación ID + PIN no es compatible.



Precaución

Si activa **Admin 2-step Authentication** y elimina las credenciales de todos los administradores hasta dejar menos de dos tipos, no podrá acceder al menú de administrador cuando BioStar X o BioStar 2 no estén disponibles. Por lo tanto, tenga especial cuidado al eliminar credenciales de administrador.

Tipo de ID de usuario

Selecciona el tipo de ID de usuario que se va a registrar en el dispositivo.

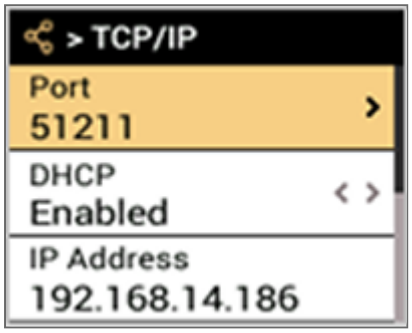
1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **DEVICE** → **User ID Type** y presione **4** o **6** para cambiar la configuración.
   - **Number**: Ingrese un ID de usuario con solo números.
   - **Alphanumeric**: Ingrese un ID de usuario con caracteres alfanuméricos y los símbolos _ -.
3. Pulsa **OK** para guardar la configuración.

Red

Cambie la configuración de comunicación de dispositivos como Ethernet, servidor y comunicación serial.

TCP/IP

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **NETWORK** → **TCP/IP** y presione **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para cambiar los ajustes.

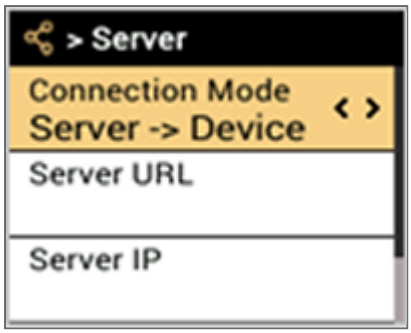


   - **PORT**: Configure los puertos del dispositivo.
   - **DHCP**: Configure si se utiliza DHCP. Si la configuración DHCP está deshabilitada, se pueden modificar **IP Address**, **Gateway** y **Subnet Mask**.
   - **IP Address**: Compruebe la dirección IP del dispositivo. Para modificarla, desactive la configuración de DHCP.
   - **Gateway**: Compruebe la puerta de enlace del dispositivo. Para modificarla, desactive la configuración de DHCP.
   - **Subnet Mask**: Compruebe la máscara de subred del dispositivo. Para modificarla, desactive la configuración de DHCP.
   - **DNS**: Establece la dirección del servidor de nombres de dominio.
4. Pulsa **OK** para guardar la configuración.

Servidor

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **NETWORK** → **Server** y presione **6**.

3. Selecciona el elemento deseado y pulsa **4** o **6** para cambiar los ajustes.

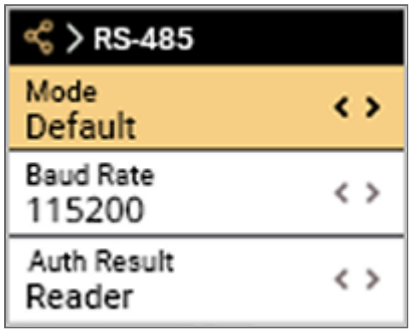


- **Connection Mode**: Al seleccionar **Device** → **Server** se envía una señal de conexión directa al servidor con la información ingresada en el dispositivo. Se pueden ingresar **Server URL**, **Server IP** y **Server Port**.
- **Server URL**: Ingrese **Server URL** en lugar de **Server IP**.
- **Server IP**: Ingrese la dirección IP de la PC donde está instalado BioStar X.
- **Server Port**: Ingrese el puerto de la PC donde está instalado BioStar X.

4. Pulsa **OK** para guardar la configuración.

Configuración de comunicación serial

1. Pulsa **ESC** y autentícate como administrador.
2. Seleccione **NETWORK** → **RS-485** y presione **6**.
3. Selecciona el elemento deseado y pulsa **4** o **6** para cambiar los ajustes.



- **Operation Mode**: Seleccione el modo de operación RS-485.
- **Baud Rate**: Seleccione el rendimiento de comunicación deseado.
- **Authentication Result**: Al usar **Intelligent Slave**, seleccione mostrar en pantalla los resultados de autenticación de controladores o dispositivos de terceros. Esta opción puede utilizarse cuando el modo de **RS-485** está configurado en **Default** o **Slave**.

4. Pulsa **OK** para guardar la configuración.

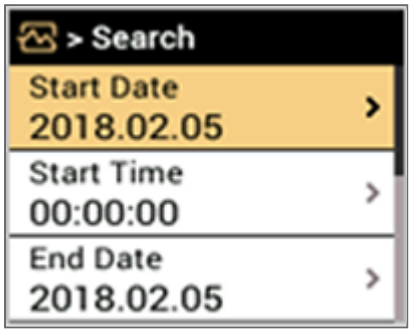
Registros de eventos

Describe cómo ver los registros de eventos generados por el dispositivo.

Busca registros de eventos

Configura condiciones para buscar registros.

1. Pulsa **ESC** y autentícate como administrador.
2. Selecciona **EVENT LOG** → **Search** y pulsa **6**.
3. Selecciona el elemento deseado y pulsa **6** para cambiar la configuración.



4. Configura las condiciones de búsqueda y pulsa **OK** para mostrar los registros que cumplen dichas condiciones.
5. Presione **ESC** para regresar a la pantalla anterior.

Eliminar todos los registros

Elimina todos los registros guardados.

1. Pulsa **ESC** y autentícate como administrador.
2. Selecciona **EVENT LOG** → **Delete All Logs** y pulsa **6**.
3. Pulsa **OK** para eliminar todos los registros. Pulsa **ESC** para cancelar.

Ver uso de registros

Consulta el estado del uso de registros.

1. Pulsa **ESC** y autentícate como administrador.
2. Selecciona **EVENT LOG** → **Log Usage** y pulsa **6**.
3. Consulta el uso de registros del dispositivo.
4. Presione **ESC** para regresar a la pantalla anterior.

Solución de Problemas

Este documento proporciona información para resolver problemas inesperados que puede encontrar al usar el dispositivo.

Verifique estos elementos antes de reportar una falla

Este documento proporciona información para resolver problemas inesperados que puede encontrar al usar el dispositivo.

Alimentación

Q. Se está suministrando energía, pero el dispositivo no funciona.

- Si el terminal y el soporte están muy separados, el dispositivo puede no funcionar debido al interruptor antisabotaje.
- Verifique el adaptador o el cable de alimentación.

PIN

Q. Perdí mi PIN.

- Para un PIN de usuario normal, solicítelo al administrador e introdúzcalo nuevamente.
- Si ha perdido el PIN de administrador, comuníquese con la empresa de instalación.

Q. Ingresé mi PIN y presioné el botón **OK**, pero aún no puedo abrir la puerta.

- Verifique si ingresó correctamente el PIN registrado.
- Verifique si cambió el PIN recientemente.
- Si no recuerda el PIN, solicítelo al administrador e introdúzcalo nuevamente.

Huella

Q. La huella se ha registrado, pero la autenticación de huella no se realiza correctamente y se producen errores con frecuencia.

- Revisa el Método correcto de ingreso de huellas dactilares y vuelve a registrar la huella.
- Si su huella tiene un corte, el dispositivo puede reconocerla como la huella de otra persona.
- Si hay muchas huellas dactilares registradas, cambie **Matching Timeout** y vuelva a intentarlo.
- La tasa de autenticación puede variar para cada huella debido a diferentes características. Registre la huella de otro dedo.

Q. La autenticación de huella dejó de funcionar repentinamente.

- Verifique si el dedo o el sensor de huella tienen sudor, agua o polvo, y límpielos.
- Seque su dedo y el sensor de huella con una toalla seca y vuelva a intentarlo.
- Si su huella está demasiado seca, sopléela y vuelva a intentarlo.

Q. El sensor de huella no se enciende.

- Cuando **Sensor Mode** está en **Auto On**, el sensor solo se encenderá al colocar el dedo sobre él. Si desea que el sensor de huella esté siempre encendido, configure **Sensor Mode** en **Always On**.

Cerradura de puerta

Q. La puerta no se bloquea al cerrarla.

- La cerradura eléctrica puede estar fallando. Solicite una inspección a la empresa de instalación.

Hora

Q. De repente, la hora es incorrecta.

- El dispositivo cuenta con una batería interna, pero si no recibe alimentación durante mucho tiempo, la batería puede agotarse y provocar que la hora sea incorrecta. Puede corregirla consultando Fecha y hora.

Acceso de administrador

Q. Perdí mi PIN de administrador, por lo que no puedo acceder al modo de administrador.

- El administrador otorga un permiso de acceso en el dispositivo, por lo que solo él puede acceder al menú de administrador.
- Si ha perdido el PIN de administrador, comuníquese con la empresa de instalación.

Administrador maestro (productos orientados a CE)

Q. ¿Es compatible la configuración de Administrador maestro después de una actualización de firmware desde un dispositivo existente?

- **Master Administrator solo es compatible en productos orientados a CE con una etiqueta con marca CE**. Use la etiqueta adhesiva en la parte posterior del producto para identificar productos **orientados a CE / globales (no CE)**. Para obtener detalles, consulte la Política de soporte del Master Administrator.

Especificaciones del Producto

Incluye las especificaciones clave del producto, como tamaño, características y rendimiento.

Credenciales

Biométrico	**Huella** • **Dimensiones de la imagen:272 x 320 píxeles** • **Profundidad de bits de la imagen:8 bits, 256 tonos de la escala de grises** • **Resolución:500 dpi** • **Plantilla:SUPREMA / ISO19794-2 / ANSI-378** • **Extractor / Comparador:Con certificación y compatible con MINEX** • **Detección de huella dactilar viva:Compatible (basado en software)**	
Tarjeta RF	**BLN2-OD, BLN2-ODB**	**125kHz EM y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa**
	BLN2-OA, BLN2-OAB, BLN2-PAB	**125kHz EM, HID Prox y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa, iCLASS SE/SR/Seos**
Rango de lectura RF[1)]	**MIFARE/DESFire/HID iCLASS: 50 mm, EM/HID Prox/FeliCa: 30 mm**	
Móvil	**BLN2-ODB, BLN2-OAB, BLN2-PAB**	**NFC, BLE**
	BLN2-OD, BLN2-OA	**NFC**

General

Nombre del modelo	**BLN2-ODB, BLN2-OAB, BLN2-PAB**
CPU	**1.2 GHz**
Memoria	**4 GB Flash + 64 MB RAM**
Chip criptográfico	**Soportado**

Visualizar	**Pantalla TFT-LCD en color de 1.77"**	
Resolución de pantalla	**160 x 128 píxeles**	
Sonido	**16 bit**	
Temperatura de funcionamiento	**BLN2-ODB, BLN2-OAB, BLN2-OD, BLN2-OA**	**De -20 °C a 50 °C**
	BLN2-PAB	**De -10 °C a 50 °C**
Temperatura de almacenamiento	**BLN2-ODB, BLN2-OAB, BLN2-OD, BLN2-OA**	**De -40 °C a 70 °C**
	BLN2-PAB	**De -20 °C a 60 °C**
Humedad de funcionamiento	**Del 0 % al 80 %, sin condensación**	
Humedad de almacenamiento	**Del 0 % al 90 %, sin condensación**	
Grado de protección IP	**IP65, IP67**	
Autenticación	**CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE**	

Capacidad

Máx. usuarios	**10,000**
Máx. credenciales (1:N)	**Huella digital: 10,000**
Máx. credenciales (1:1)	• **Huella dactilar: 10,000** • **Tarjeta: 10,000** • **PIN: 10,000**
Máx. registros de texto	**1,000,000**

Interfaz

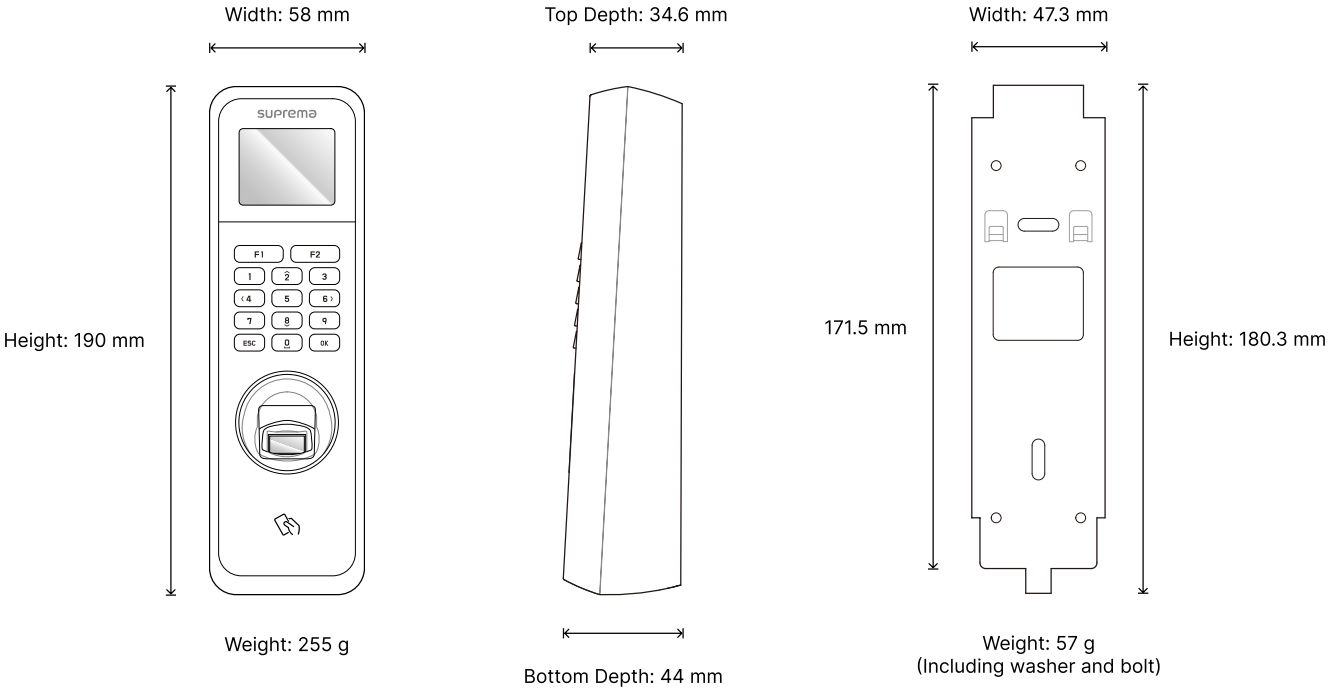
Ethernet	**Compatible (10/100 Mbps, MDI/MDI-X automática)**
Protocolo de red	**TCP, UDP**
RS-485	**1 canal maestro/esclavo (seleccionable)**
Protocolo de comunicación RS-485	**Compatible con OSDP V2**
Wiegand	**Entrada o salida de 1 canal (seleccionable)**
Entrada	**2 canales de entrada**
Relé	**1 relé**
Tamper	**Soportado**

Eléctrico

Alimentación	**12 Vdc**	**Corriente: Máx. 0.4 A**
Entrada de interruptor VIH	• **Mín.: 3 V** • **Máx.: 5 V**	
Entrada de interruptor VIL	**Máx.: 1 V**	
Resistencia pull-up del interruptor	**4.7 kΩ (los puertos de entrada se polarizan con 4.7 kΩ)**	
Salida Wiegand VOH	**Más de 4.8 V**	
Salida Wiegand VOL	**Menos de 0.2 V**	
Resistencia pull-up de salida Wiegand	**Polarización interna de 1 kΩ**	

Relé	• **Carga resistiva de 2 A a 30 VCC** • **Carga inductiva de 1 A a 30 VCC**

Dimensiones y peso



1) El rango de detección de RF puede variar según el entorno de instalación.

Información

Las especificaciones del producto están sujetas a cambios sin previo aviso para mejorar el rendimiento.

Información Reglamentaria

Proporciona información sobre las normativas y certificaciones que cumple el producto.

Información de cumplimiento de la FCC

ESTE DISPOSITIVO CUMPLE CON LA PARTE 15 DE LAS NORMAS DE LA FCC.

El funcionamiento está sujeto a las siguientes dos condiciones:

1. Este dispositivo no debe causar interferencias perjudiciales, y
2. Este dispositivo debe aceptar cualquier interferencia recibida, incluida la interferencia que pueda causar un funcionamiento no deseado.

Información

Este equipo ha sido probado y se determinó que cumple con los límites para un dispositivo digital Class A, de conformidad con la parte 15 de las normas de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias perjudiciales cuando el equipo se opera en un entorno comercial. Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con el manual de instrucciones, puede causar interferencias perjudiciales en las comunicaciones por radio. El funcionamiento de este equipo en un área residencial probablemente cause interferencias perjudiciales; en tal caso, se requerirá que el usuario corrija la interferencia a su propio costo.

Cualquier cambio o modificación que no esté expresamente aprobado por la parte responsable del cumplimiento podría anular la autoridad del usuario para operar este equipo.

Este transmisor no debe colocarse ni operar junto con ninguna otra antena o transmisor.

Este equipo cumple con los límites de exposición a radiación establecidos por la FCC para un entorno no controlado. Este equipo debe instalarse y operarse manteniendo una distancia mínima de 20 cm entre el radiador y su cuerpo. No instale ni opere este dispositivo y su antena junto con ninguna otra antena o dispositivo de transmisión RF.

Información de IC

Este dispositivo cumple con las RSS exentas de licencia de Industry Canada.

El funcionamiento está sujeto a las siguientes dos condiciones:

1. Este dispositivo no debe causar interferencias, y
2. Este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan causar un funcionamiento no deseado.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage ;
2. l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Declaración de conformidad de la UE (CE)

Este producto cuenta con la marca CE conforme a las disposiciones de la Directiva de Equipos Radioeléctricos (RED) 2014/53/UE.

Por la presente, Suprema Inc. declara que este producto cumple con los requisitos esenciales y otras disposiciones pertinentes de la Directiva de Equipos Radioeléctricos (RED) 2014/53/UE y lleva la marca CE. Este dispositivo es un equipo de radio Clase 1 según las instrucciones.

- Potencia de transmisión Bluetooth: -7.9 dBm
- Frecuencia Bluetooth: 2402~2480 MHz
- Frecuencia NFC: 129.2 MHz
- Frecuencia RFID: 13.56 MHz

Para obtener más información, contáctenos mediante los datos de contacto a continuación.

Suprema Inc.

Dirección: 17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. de COREA

Tel.: +82-31-783-4502 / Fax: +82-31-783-4503

Apéndices

Incluye avisos legales contenidos en el producto.

Descargos de responsabilidad

- La información de este sitio web se proporciona en relación con los productos de Suprema.
- El derecho de uso se reconoce únicamente para los productos de Suprema incluidos en los términos y condiciones de uso o venta de dichos productos garantizados por Suprema. Este sitio web no otorga ninguna licencia, expresa o implícita, por impedimento legal ni de ningún otro tipo, sobre ninguna propiedad intelectual.
- Salvo lo expresamente establecido en un acuerdo entre usted y Suprema, Suprema no asume ninguna responsabilidad y rechaza toda garantía, expresa o implícita, incluidas, entre otras, las relativas a la idoneidad para un fin particular, la comerciabilidad o la no infracción.
- Todas las garantías quedan ANULADAS si los productos de Suprema han sido: 1) instalados incorrectamente o si los números de serie, la fecha de garantía o las etiquetas de control de calidad del hardware han sido alterados o retirados; 2) utilizados de una manera distinta a la autorizada por Suprema; 3) modificados, alterados o reparados por un tercero que no sea Suprema o un tercero autorizado por Suprema; o 4) operados o mantenidos en condiciones ambientales inadecuadas.
- Los productos de Suprema no están destinados a usos médicos, de salvamento, de soporte vital ni a otras aplicaciones en las que la falla del producto de Suprema pudiera ocasionar lesiones personales o la muerte. Si compra o utiliza productos de Suprema para cualquiera de estas aplicaciones no previstas ni autorizadas, deberá indemnizar y eximir de responsabilidad a Suprema y a sus directores, empleados, subsidiarias, afiliadas y distribuidores por todos los reclamos, costos, daños y gastos, incluidos los honorarios razonables de abogados, derivados directa o indirectamente de cualquier reclamo por lesiones personales o muerte asociado con dicho uso no previsto o no autorizado, incluso si el reclamo alega que Suprema fue negligente en el diseño o la fabricación de la pieza.
- Suprema se reserva el derecho de realizar cambios en las especificaciones y descripciones de los productos en cualquier momento y sin previo aviso para mejorar la confiabilidad, la función o el diseño.
- La información personal, en forma de mensajes de autenticación y otra información relacionada, puede almacenarse en los productos de Suprema durante su uso. Suprema no se hace responsable de ninguna información, incluida la información personal, almacenada dentro de los productos de Suprema que no esté bajo el control directo de Suprema o según lo establecido en los términos y condiciones correspondientes. Cuando se utilice cualquier información almacenada, incluida la información personal, es responsabilidad de los usuarios del producto cumplir con la legislación nacional (como el RGPD) y garantizar su manipulación y tratamiento adecuados.
- No debe confiar en la ausencia o las características de ninguna función o instrucción marcada como "reservada" o "indefinida". Suprema las reserva para su definición futura y no tendrá ninguna responsabilidad por conflictos o incompatibilidades derivados de cambios posteriores en ellas.
- Salvo que se disponga expresamente en el presente documento y en la medida máxima permitida por la ley, los productos de Suprema se venden "tal cual".
- Comuníquese con la oficina de ventas local de Suprema o con su distribuidor para obtener las especificaciones más recientes y antes de realizar su pedido.

Aviso de derechos de autor

Los derechos de autor de este sitio web pertenecen a Suprema. Los derechos sobre otros nombres de productos, marcas comerciales y marcas registradas pertenecen a las personas u organizaciones propietarias.

Licencia de código abierto

- El software de este producto se creó modificando la versión 4.x del kernel de Linux y la licencia del kernel de Linux se rige por la GPL. Para obtener más información sobre la licencia GPL, consulte la GNU General Public License.
- La biblioteca glibc incluida en este producto se rige por la LGPL. Para obtener más información sobre la licencia LGPL, consulte la GNU Lesser General Public License.
- La biblioteca QT incluida en este producto se rige por la LGPL. Para obtener más información sobre la licencia LGPL, consulte la GNU Lesser General Public License.
- Este producto usa "OpenSSL", que está licenciado bajo las licencias OpenSSL y Original SSLeay. Para más información sobre las licencias OpenSSL y Original SSLeay, consulte la OpenSSL License y la Original SSLeay License.
- El código fuente modificado basado en el kernel de Linux 4.x, la biblioteca glibc y la biblioteca QT incluidas en este producto puede descargarse contactando al Equipo de Soporte Técnico de Suprema.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

Para obtener más información sobre las sucursales globales de Suprema,
visite la página web a continuación escaneando el código QR.
http://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema Inc. Suprema y los números y los nombres que identifican productos mencionados en este documento son marcas comerciales registradas de Suprema, Inc. Todas las marcas y los nombres de productos que no pertenecen a Suprema son marcas comerciales o marcas comerciales registradas de sus respectivas compañías. La apariencia del producto, el estado de la estructura o las especificaciones están sujetas a cambio sin previo aviso.